Le Cloud Computing

Une opportunité pour l'économie en Belgique

economie
SPF Economie, P.M.E., Classes moyennes et Energie

.be

Le Cloud Computing

Une opportunité pour l'économie en Belgique

Service public fédéral Economie, P.M.E., Classes moyennes et Energie
Rue du Progrès 50
1210 Bruxelles
N° d'entreprise : 0314.595.348
http://economie.fgov.be

tél. 02 277 51 11

Pour les appels en provenance de l'étranger :
tél. + 32 2 277 51 11

Editeur responsable : Jean-Marc Delporte
Président du Comité de direction
Rue du Progrès 50
1210 Bruxelles

Version internet

E9-1055/0369-13

Avis

Ce rapport a été rédigé pour le SPF Economie, P.M.E., Classes moyennes et Energie par Unisys Corporation. Il reflète l'opinion de ses auteurs, basé sur les sources citées. Le SPF Economie ni les auteurs ne peuvent être rendus responsables de l'usage qui pourrait être fait du contenu de ce rapport.

Auteurs :

UNISYS

Patrice-Emmanuel Schmitz – expert juridique, directeur des études européennes

Giedré Kazlauskaite – Sr consultante juridique

Michel Hoffmann – Sr consultant en matière de sécurité

Pierre Franck – Sr consultant en technologies de l'information

Table de Révisions

Ver.	Date	Auteur	Description	Action*	Page(s)
0.1 – 0.3	15.03.2013	Tous	Première version interne	I	Toutes
0.4	04.04.2013	Tous	Draft version finale	I	Toutes
1.0	05.04.2013	Tous	Version finale envoyée au SPF Economie	I	Toutes
1.1	30.04.2013	Tous	Version incluant les corrections du SPF ainsi que les points discutés lors de la présentation du 25 avril 2013	I	Toutes
1.2	08.05.2013	Tous	Version finale revue par le SPF Economie	I	Toutes

(*) Action: I = Insertions R = Replacement

Table des matières

Liste des figures

Liste des tableaux

1 Introduction

Le présent document est le rapport final d'une étude sur le « *cloud* computing » (pour des facilités de traduction, nous utiliserons ce terme plutôt que « informatique en nuage »). Cette étude a été commandée à Unisys par le Service public fédéral Economie, P.M.E., Classes moyennes et Energie (SPF Economie)[1].

On perçoit souvent le *cloud computing* comme étant l'enregistrement de données sur des serveurs d'un hébergeur externe. Les informations sauvegardées par le biais du *cloud computing* sont consultables grâce à différents outils électroniques et une connexion internet. Dans ce cadre, nous pensons principalement à l'utilisation croissante des tablettes et des smartphones, mais cela n'exclut pas d'autres matériels plus lourds comme les PC et serveurs d'entreprises ou départementaux qui utiliseraient le *cloud* à des fins de centralisation, consolidation ou sauvegarde.
Actuellement, de nombreuses applications « grand public » ont déjà recours au *cloud computing* : Hotmail, i*Cloud*, Facebook, … Par conséquent, nombreux sont ceux, principalement parmi les citoyens de la « jeune génération Y », qui utilisent déjà cette technologie sans vraiment y prêter attention et l'utiliseront tout naturellement plus tard lorsqu'ils seront responsables dans une entreprise ou dans un service public.

Pourtant, malgré les avantages économiques et techniques évidents des services offerts, tant pour les entreprises que pour les particuliers, l'activité du *cloud* n'a pas encore atteint sa maturité. Le manque de confiance relatif à la sécurité et à la fiabilité du système, ainsi que dans le caractère équitable et pérenne des relations avec les fournisseurs en sont les principales raisons. Certains ne sont pas loin de considérer le *cloud* comme une nouvelle féodalité, dans laquelle le vassal se soumet à son suzerain (acceptant de subir ses règles, messages et publicités) et le seigneur, en échange, se déclare gardien des droits du vassal et le couvre de sa haute protection. Dans cette vision pessimiste, les clients auraient pour principale liberté celle de « choisir leur maître » et ils deviennent eux-mêmes une sorte de marchandise : un cheptel d'affiliés captifs[2]. A ce déséquilibre contractuel s'ajoute l'insécurité juridique car les hébergeurs des données du *cloud*, les lieux mobiles où se situent les serveurs sont changeants et souvent localisés dans des pays où les règles en matière de sécurité des données et de protection de la vie privée sont moins strictes, avec le risque réel ou supposé que quelqu'un s'autorise à prendre connaissance de documents confidentiels à l'insu de leur propriétaire légitime.

Il faut donc sensibiliser toutes les parties prenantes, aussi bien les autorités de régulation que les opérateurs économiques du *cloud* et leurs clients (les services publics, les entreprises grandes et petites, les citoyens) quant à la nécessité de mettre en place un cadre juridique efficace et de grande qualité pour le *cloud*

[1] Dans la Belgique fédérale, la notion de SPF est équivalente à la notion de « ministère » dans les autres Etats membres de l'Union européenne.
[2] Wired opinion: When It Comes to Security, *We*'re Back to Feudalism
www.wired.com/opinion/2012/11/feudal-security

computing. Grâce à ce cadre, et le cas échéant aux labels visibles qui en signaleraient l'application, les utilisateurs du système comprendraient qu'ils opèrent selon des modalités « les plus justes possible » (fair trade ou commerce équitable) sur le plan contractuel et « les plus sûres possible compte tenu des progrès de l'état de l'art » sur le plan de la sécurité et de la protection des données.

L'étude s'est déroulée selon les priorités suivantes :

- Analyser les notions, avantages et risques du *cloud* computing
  1. La notion de *cloud computing* (définition et attributs)
  2. Les risques et opportunités (ou avantages) du *cloud computing*
  3. Quels impacts peut-on attendre du développement du *cloud computing* ?
  4. Quel est le marché du *cloud computing* en Belgique et en Europe ?
- Analyser les aspects juridiques et les clauses contractuelles à recommander
  1. Compte tenu de ce qui existe en droit belge
  2. Compte tenu des réformes entreprises sur le plan européen
- Evoquer les mesures à prendre, par les acteurs privés, publics et par le SPF Economie.

Le rapport intermédiaire de décembre 2012 s'est concentré sur la première priorité, tandis que les deuxième et troisième priorités sont traitées dans ce rapport, après concertation avec des représentants de la Commission européenne et avec les acteurs locaux du *cloud computing* en Belgique (réunions de décembre 2012 et de février 2013).

Il faut signaler qu'entre le moment où l'étude a été attribuée (été 2012) et le moment de la rédaction du rapport final (les trois premiers mois de 2013), nous avons vu la publication de nombreuses prises de position et rapports de la part de la Commission européenne, des agences spécialisées de l'Union européenne, de groupes d'experts et d'Etats membres. La matière est donc très mouvante, les « grands Etats » ont tendance à se reposer sur leur marché et à progresser sans attendre une dynamique communautaire. Ceci renforce la difficulté pour des Etats plus petits, qui n'ont pas le même marché intérieur (notamment public) et dont la prise de décision est fragmentée, de se définir une voie innovante et autonome.

2 Résumé

Le *cloud computing* est ***l'accès à des ressources informatiques sur demande par l'intermédiaire d'un réseau***.

C'est donc principalement un service dans lequel le client (l'utilisateur du *cloud*) utilise à distance des ressources qui lui sont fournies (plutôt que de tout installer localement chez lui).

Il y a plusieurs modèles de déploiement du service : privé (si le client est seul utilisateur des ressources qui lui sont dédiées), partagé (avec une communauté plus ou moins grande), public (quand le service est proposé à tous), étant entendu que ces modèles peuvent se mélanger de façon hybride.

Le service lui-même peut couvrir ou combiner diverses offres : l'infrastructure assurant calcul, stockage, back-up, bande passante (IaaS), la plateforme d'exploitation (PaaS) permettant enfin d'offrir en ligne des applications ou logiciels (SaaS) qui permettent de traiter des données.

Le principe économique du *cloud* est que le client évite les gros investissements en capitaux requis pour créer et maintenir une informatique de pointe (il peut avantageusement se consacrer à développer sa mission spécifique) et ne paie les services (coûts opérationnels) que s'il en a besoin et au moment où il en a besoin. Il faut aussi signaler que certains services, principalement destinés au grand public, sont « gratuits en contrepartie de publicité », comme le courrier électronique, les réseaux sociaux ou la recherche sur internet.

Le principe contractuel du *cloud*, au fur et à mesure que l'on va du « *cloud* privé » au « *cloud* partagé ou public » va d'un contrat négocié à un contrat par adhésion (dans lequel les conditions sont à prendre ou à laisser, et peuvent parfois même être modifiées unilatéralement par le fournisseur), ce qui renforce la nécessité de mettre en place un « cadre équitable ».

Le principe technique du *cloud*, qui est l'utilisation à distance, suppose la mobilité des données (dans les centres de calcul du fournisseur qui disposent au moment voulu de la puissance requise) et peut donc induire une perte de contrôle du client sur le lieu exact où elles sont conservées.

Les avantages du *cloud,* en plus de la création de nouveaux emplois dans les zones d'installation des centres de calcul (nouvelle branche d'activité compensant certaines pertes d'emploi ou réorientations au sein des clients) découlent de son principe économique et comprennent en outre pour les clients une meilleure gestion/attribution des coûts de chaque tâche, une agilité de prise décision (sans délais ni gestion prévisionnelle), une meilleure résistance face aux menaces cybernétiques et/ou sinistres (incendies, inondations, vols) qui peuvent affecter une informatique isolée, localisée en un seul point.

Les risques n'ont cependant pas disparu et – du fait de la taille des centres qui peuvent héberger les données de milliers de clients, soit de pans entiers d'une économie - ils ont pris une nouvelle dimension avec le *cloud.* La section 4 de cette étude les analyse selon le modèle de service (IaaS, PaaS, SaaS) et de déploiement (privé, public, hybride) et propose une approche d'évaluation des risques, de revue des politiques de sécurité du client, de traitement des risques et d'usage contrôlé du *cloud* avec des vérifications périodiques.

Le marché du *cloud* a fait, durant l'année écoulée, l'objet d'études nombreuses : il serait en croissance forte, passant en Europe, pour le *cloud* public ou communautaire de 4,6 milliards d'euros (2011) à 6,2 milliards d'euros pour 2012 (soit 33 % pour cette seule année). La part belge de ce marché est estimée à 2,5 %, soit 153 millions en 2012. La croissance peut avoir un aspect conjoncturel (les entreprises sont en recherche d'économies) et son maintien ou son évolution dépendra autant de la situation économique globale (reprise, sortie de crise ou non), que de l'absence d'incidents majeurs (pas de publicité négative) et de la dissipation des freins, incertitudes et manques de confiance vis-à-vis du *cloud*.

C'est dans ce dernier domaine que l'autorité régulatrice peut jouer un rôle important, selon qu'elle (et les opérateurs concernés) collabore on non pour adopter un cadre juridique assurant une confiance forte du marché. On peut tracer trois scénarios : pessimiste, linéaire ou optimiste, selon lesquels le marché belge n'évoluerait d'ici 2020 que modérément (880 millions d'euros), linéairement (1,5 milliards d'euros) ou plus fortement (2 milliards d'euros en 2020).

Comment définir ce nouveau cadre juridique ? Les lois actuelles n'ont pas été formulées en tenant compte du *cloud* computing, et – au moins depuis la directive 95/46 – elles découlent du droit européen, ce qui fait que l'intérêt pour un Etat membre de légiférer seul est limité. Si les rôles des partenaires du *cloud* (client et fournisseur) peuvent déjà être déduits du droit actuel (responsable du traitement et sous-traitant), le droit relatif au *cloud* va être influencé par une série de réformes européennes ou d'actions en cours :

- Un nouveau règlement général sur la protection des données (projet dévoilé en 2012) ;
- Une adaptation des droits du consommateur de confier au *cloud* ses copies privées et d'obtenir des clauses contractuelles équitables ;
- Une adaptation des règles relatives au commerce électronique et à la gestion du « contenu illégal » constaté sur le *cloud ;*
- Une définition des standards du « *cloud* européen » sur le plan technique (pour en assurer la portabilité), contractuel (pour un SLA équitable) et de la sécurité (rapport d'incidents, mesures et audit) ;
- Un « partenariat européen pour le *cloud* » qui vise non à construire un « super centre de *cloud* européen » mais à définir ces règles et standards communs permettant d'harmoniser les spécifications (notamment du secteur public) et les droits face aux offres des fournisseurs.

Toutes ces réformes ou actions (parfois devancées de manière fort isolée par les initiatives purement nationales de certains Etats) seront ponctuées d'études et de rapports (dont plusieurs sont en cours d'élaboration et attendus en 2013-14). Elles ne seront pas appliquées du jour au lendemain, mais cela prendra des années.

Que peut donc faire l'autorité régulatrice belge ?

Elle doit d'abord s'inscrire dans l'approche européenne, pratiquant à cet égard une veille technologique, élaborant des documents de synthèse qui soient rapidement évolutifs, et en déclarant son ouverture à toute approche de mutualisation (pooling) de projets *cloud* avec les services publics de ses voisins.

Il faut que s'établisse une relation de collaboration avec les représentants de la profession du *cloud*, qui eux-mêmes doivent encore parvenir à une meilleure organisation, plus structurée et représentative de l'ensemble du secteur à travers les différentes régions et spécialisations.

Il peut déjà être utile de devancer les conclusions attendues dans le cadre d'études en cours et du partenariat européen pour le *cloud* et élaborant, sur base des travaux de la Commission, de cette étude et des travaux du groupe de travail « Article 29 » une liste de référence des conditions contractuelles équitables et par le lancement d'un label « Fair *Cloud* » dont les adhérents pourraient se prévaloir.

La publication d'une « liste-test » (check list) relative aux points à vérifier avant d'entreprendre une migration vers le *cloud* est également souhaitable car, tout en informant efficacement le public, cela contribuera à harmoniser les conditions offertes par les fournisseurs.

Enfin, en matière de sécurité, l'autorité régulatrice, se fondant sur les recommandations de l'ENISA, devrait mettre en place et faire contrôler un cycle de rapport obligatoire des incidents (selon certaines limites ou ordre de gravité), d'estimation des risques qui peuvent en découler et de mise en place de mesures pour réduire et annuler ces risques.

3 Qu'est-ce que le *cloud* computing ?

3.1 Une informatique distribuée

Le *cloud computing* est un terme à la mode, abondamment utilisé de nos jours, pour décrire un éventail de technologies.
Il est donc important d'en définir la notion, les limites et d'identifier ce qu'il peut avoir d'innovant par rapport aux pratiques déjà anciennes d'infogérance.

De manière générale, on dira que le *cloud computing* est ***l'accès à des ressources informatiques sur demande par l'intermédiaire d'un réseau***.

En d'autres termes, dans une entreprise « abonnée au *cloud* », l'informatique serait distribuée exactement comme l'eau, le gaz ou l'électricité : il suffit de se brancher pour en bénéficier, la facture se fait selon la consommation et durant les périodes de non-utilisation (les congés, les vacances), on peut simplement fermer le compteur.

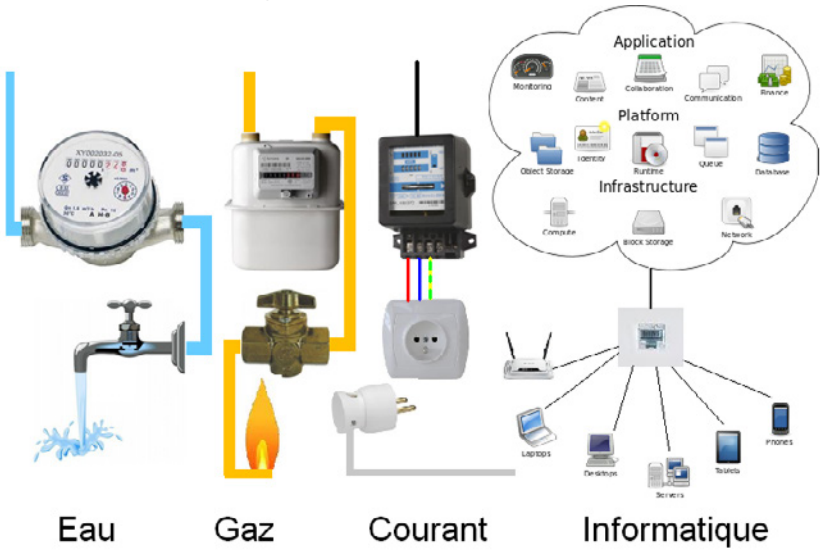

Figure 1 – Le cloud illustré

Au-delà de cette définition très générale, il est pratique de définir le *cloud computing* par ses modèles de déploiement, ses modèles de services et ses autres attributs caractéristiques.

3.2 *Divers modèles de déploiement*

On distingue le c*loud* privé (réservé à un client) du c*loud* public (proposé à tous). Entre les deux, on trouve des modèles dits « communautaires », « hybrides » ou même « souverains ».

3.2.1 *Cloud* privé

Ce modèle est très proche de l'infogérance (ou « outsourcing ») classique : le client est le seul utilisateur du service qui lui est dédié. Le matériel (hardware : les serveurs, dispositifs de copie, pare-feu etc.) peut être opéré et maintenu par un fournisseur de *cloud* aux termes d'un contrat d'outsourcing. L'accès aux ressources peut être limité au personnel du client, par un réseau local physique ou virtuel (wide area network). Dans ce modèle, le contrat peut souvent être négocié (adapté aux besoins spécifiques du client).

3.2.2 *Cloud* communautaire

Un groupe de clients accèdent aux ressources d'un même fournisseur. En général, il s'agit de répondre à des besoins particuliers comme le respect de dispositions légales ou un niveau de sécurité déterminé. Ce groupe peut être ouvert à des nouveaux venus partageant les mêmes besoins. L'accès aux ressources ainsi mises en commun est généralement restreint aux utilisateurs du réseau (wide area network).

3.2.3 *Cloud* public

Une infrastructure, une plateforme et des logiciels sont mis en place et gérés par le fournisseur de *cloud*, qui invite le grand public (des entreprises, des clients ou des utilisateurs finaux) à utiliser ce service. Ce peut être gratuit dans une certaine mesure, ou payant. L'accès au service se fait généralement par internet.

3.2.4 *Cloud* hybride

Le *cloud* hybride désigne une combinaison de *cloud*s privé, communautaire et public. Un client peut alors répartir données et accès aux applications de traitement entre les différents types de *cloud*, cet accès pouvant être plus ou moins restrictif selon les cas.

Il est également possible et souvent inévitable de combiner les divers services *cloud* externes (publics et/ou privés) et une infrastructure interne. Il est évident qu'un modèle totalement externe est irréaliste pour la majorité des entreprises dont le fonctionnement repose sur une informatique de production lourde qui n'a pas été conçue à l'origine pour tirer profit des possibilités du *cloud*. Le modèle hybride s'impose donc souvent et les entreprises doivent s'attendre à des investissements conséquents afin d'intégrer les services internes et externes, privés et publics. La capacité de gérer un environnement hybride fera la différence entre réussite et échec.

3.2.5 Autres catégories : *cloud* souverain (?)

On a évoqué aussi d'autres catégories comme ce que l'on a appelé le « *cloud* souverain [3]», qui combine les *cloud*s public et communautaire à l'échelle d'un pays, afin notamment de se rattacher à un cadre juridique et économique déterminé. On ne sera pas trop étonné d'apprendre que le gouvernement français a chargé sa Caisse des Dépôts d'encadrer un appel à projets où elle se retrouve elle-même partenaire dans divers consortiums formés par des entreprises françaises[4]. Cette initiative est censée constituer une alternative aux offres des acteurs américains et garantir la souveraineté des données des administrations et entreprises françaises, en présumant que seul un acteur français du *cloud* (et sous le contrôle direct du gouvernement) peut mettre en œuvre sur le territoire national des infrastructures qui garantissent que les données stockées resteront en sécurité sur le territoire national. Bien que les règles d'éligibilité des projets n'excluent pas formellement les entreprises « non-françaises » et se réfèrent aux règles coopératives européennes, il est clair qu'un tel concept suscite des questions par rapport au droit communautaire[5] et s'est vu critiqué de l'intérieur, notamment par les filiales françaises d'entreprises étrangères.

3.3 Divers modèles de service

On peut utiliser le *cloud computing* pour fournir un grand nombre de solutions, mais il y a essentiellement trois grands types de service : l'infrastructure, la plateforme et les applications (ou logiciels, ou software).

[3] Expression utilisée notamment par Isabelle Renard (avocate – cabinet Racine) pour désigner le « cloud français » - Le cloud computing en France – 16 octobre 2012 (exposé).

[4] Sous le thème « Investissements d'Avenir, Développement de l'Economie Numérique », cet appel clôturé le 2 novembre 2011 a permis plusieurs initiatives dans lesquelles les autorités françaises sont partenaires : principalement les consortiums Numergy (Caisse des dépôts, SFR, Bull) et CloudWatt (Caisse des dépôts, Orange, Thales) qui a donné naissance à une société commerciale résultant d'un partenariat public-privé: Andromède.

[5] IBM France a rapidement fait état d'une « distorsion de concurrence, trouvant que l'Etat fait ici supporter des investissements technologiques par les contribuables, ce qui lui permettra par la suite d'appliquer une baisse artificielle des prix » - les Echos - http://archives.lesechos.fr/archives/2012/lesechos.fr/01/31/0201873061845.htm.
Pour de toutes autres raisons, certains acteurs français se sont interrogés sur le fait que l'Etat français puisse être actionnaire à part égale dans deux structures concurrentes (initialement membre du projet formé avec SFR, Dassault Systèmes s'en est finalement retiré à cause de cette dualité, alors qu'un seul projet lui semblait préférable http://www.latribune.fr/technos-medias/20120405trib000692197/dassault-systemes-claque-la-porte-du-cloud-a-la-francaise.html).

3.3.1 L'infrastructure (IaaS ou « Infrastructure as a Service »)

L'offre donne un accès partagé à une grande puissance de calcul, ou de stockage, ou de communication. Plutôt que de devoir acquérir toute cette puissance (dont il n'a sans doute besoin que de manière épisodique, périodique ou pour des tests momentanés), le client achète un accès qui lui fournira toute la puissance, l'espace ou la rapidité de communication nécessaire au moment voulu.

3.3.2 La plateforme (PaaS ou « Platform as a Service »)

L'offre donne accès à une plateforme de développement : un environnement spécifique qui permet à l'utilisateur d'écrire et de tester des applications qui tourneront sur cette plateforme ou sur une installation similaire. C'est le cas par exemple d'un réseau social ou d'un constructeur qui offre une plateforme qui permet à des développeurs de créer des applications spécialement destinées à interagir avec ce réseau, avec l'écosystème ou l'univers fonctionnel de ce constructeur.
La plateforme (middleware) définit les standards qui permettront de s'adresser de manière large et interopérable à de nombreux clients et d'élargir leur choix en matière de logiciel. Il est clair que ce service PaaS peut être hébergé sur une infrastructure IaaS.

3.3.3 Le logiciel (SaaS ou « Software as a Service »)

L'offre donne accès à une application complète et opérationnelle à laquelle l'utilisateur accède au moyen de son navigateur Web ou d'un autre logiciel client. Cette manière d'utiliser du logiciel élimine ou réduit fortement le besoin d'installer des programmes sur chaque poste client. De plus, le service est généralement accessible à une gamme la plus étendue possible de matériels : PC, tablettes, téléphones etc. Cela permet par exemple à une jeune start-up d'utiliser un puissant logiciel de gestion de clientèle, qu'elle n'aurait pas pu acquérir pour son usage exclusif.

Bien sûr, ce service SaaS peut être aussi hébergé sur une plateforme PaaS et une infrastructure IaaS, ce qui fait aussi que l'on peut avoir différents contrats et différents fournisseurs « en cascade » pour chaque couche : une compagnie A peut offrir l'accès à un logiciel qu'elle a acheté à une compagnie B, qui utilise les standards de la plateforme C et qu'elle fait tourner sur une infrastructure opérée par une compagnie D.

3.4 Divers modes de financement

Une caractéristique du *cloud computing* est le paiement des fournitures « selon la consommation ». Cependant il existe une série de services qui sont, jusqu'à présent, soit toujours gratuits (comme la consultation de l'internet via un moteur de recherche), généralement gratuits (comme l'accès de base à un réseau social) soit proposés gratuitement dans certaines limites de volume ou de pages (comme le courrier ou l'agenda électronique). Les services « gratuits » ne peuvent se financer que par la publicité ou par l'utilisation du profil même de leurs utilisateurs comme « capital commercialisable ». Il en résulte que le service gratuit n'est viable à long terme que s'il sert d'attraction ou de support pour d'autres activités et s'il parvient à concentrer ou réunir une masse énorme d'utilisateurs : le *cloud computing* gratuit, destiné au grand public, est par excellence un domaine où le potentiel de concentration aux mains de quelques acteurs dominants est extrême.

3.5 Des caractéristiques spécifiques au cloud

Comme une définition générale du *cloud computing* ne peut être qu'assez vague, on peut se référer à ses principales caractéristiques, dont certaines ont déjà été évoquées plus haut, d'autres étant nouvelles.

3.5.1 Caractéristiques de base :

- Le client du *cloud* accède avec son périphérique (ordinateur de bureau, portable, tablette, téléphone, serveur en ligne) à trois couches de services (infrastructure, plateforme, applications) ;
- A l'exception des périphériques, l'infrastructure, les plateformes, les applications sont propriété du fournisseur de *cloud*, non de l'utilisateur ;
- L'utilisateur interagit avec les services par un réseau, le plus souvent par internet. Les données sont donc distantes : leur support de stockage ne se trouve plus sous le contrôle direct de l'utilisateur ;
- L'accès se fait de n'importe où (la localisation du périphérique n'a pas d'importance) ;
- L'accès se fait à n'importe quel moment. Il n'y a pas d'heures « de bureau » ou « de travail » par rapport à des périodes de repos ou d'indisponibilité. Comme c'est le cas pour l'eau ou l'électricité, la disponibilité de l'infrastructure est normalement constante ;
- L'infrastructure distante stocke les données tandis que des applications logicielles en permettent l'accès ou le traitement ;
- L'utilisation des logiciels fournis pour l'accès et le traitement des données se fait à la demande ;

- Le paiement des services se fait normalement selon l'usage (sur base des volumes transférés, de l'espace disque, du nombre d'utilisateurs), ce qui évite aux nouveaux clients de devoir supporter l'ensemble des coûts qui résulteraient d'une exclusivité. Certaines entreprises donnent au grand public des accès totalement gratuits (mais limités en volume) qu'elles financent par la publicité.

3.5.2 Eléments nouveaux

Il y a cependant d'autres caractéristiques, spécialement importantes, qui marquent une différence par rapport à l'infogérance (ou outsourcing) classique :

- **La mouvance géographique**
  L'usage des services, et particulièrement de l'infrastructure, est optimisé dynamiquement dans un réseau de serveurs, ce qui fait que la localisation des données et de la machine qui en assure le traitement à un temps donné est souvent fluctuante (et inconnue de l'utilisateur, qui en général n'a pas à s'en soucier). Cette répartition dynamique correspond à une certaine nécessité. Une distribution vraiment « mondiale » de l'infrastructure en réseau sera la plus efficace pour la simple raison que – du fait de la rotation de la terre et de différentes cultures ou besoins – les uns travaillent à l'heure de pointe tandis que d'autres dorment, dînent, ne font rien ou fort peu de choses. La conséquence est que les opérateurs sont amenés à migrer constamment les charges de travail d'un centre de traitement à un autre pour une utilisation optimale du matériel. Cela ne sera pas sans influence sur le régime juridique applicable au traitement.
- **La flexibilité**
  C'est la capacité d'adapter constamment le service (infrastructure, plateforme et applications) à des besoins fluctuants, comme par exemple la quantité de données à traiter par une application, le nombre d'utilisateurs simultanés qui peuvent interagir, etc… On peut sur ce point distinguer la faculté d'adaptation dite « horizontale » (qui se réfère au nombre des transactions ou requêtes à traiter) et « verticale » (qui se réfère à la taille de ces transactions).
- **Le partage**
  A la différence de l'infogérance classique, les ressources sont mises en commun pour servir à un nombre fluctuant et indéterminé de « consommateurs ». Le comportement de certains a évidemment une influence sur les performances que les autres peuvent obtenir, étant donné que les ressources physiques et virtuelles sont constamment assignées et réassignées selon la demande.
- **Des pratiques contractuelles spécifiques**
  Sur le plan des contrats qui peuvent être établis entre le fournisseur de *cloud* et l'utilisateur, on retrouve les caractéristiques de l'infogérance ou outsourcing : un contrat de service récurrent, qui consiste à confier à un tiers tout ou partie de la gestion de son système d'information.

Toutefois, plus on progresse du « *cloud* privé » (sur mesure) vers le « *cloud* public », plus le contrat est un contrat d'adhésion, c'est-à-dire une liste de conditions à prendre ou à laisser. A la limite, l'adhésion se borne à marquer son accord, par un clic de souris dans une check box « J'accepte vos conditions ».

Bien plus, il arrive que le fournisseur de *cloud* se réserve alors le droit de modifier unilatéralement les conditions du contrat, l'utilisateur étant alors plus ou moins informé, renouvelant tacitement son adhésion selon le principe « qui ne dit mot consent ».

Ces caractéristiques écartent le *cloud* du contrat d'infogérance classique qui comporte généralement des clauses permettant :

- La mesure du niveau de service, régulièrement rapportée à l'utilisateur ;
- L'audit indépendant des performances, sur demande ;
- Des pénalités en cas de performance insuffisantes ;
- Des garanties de réversibilité.

Il est bon de noter que le fournisseur de *cloud* est souvent dans l'incapacité technique d'agir autrement. On se retrouve ici dans un cas similaire à la distribution d'eau, de gaz ou d'électricité : quand une infrastructure est partagée par des milliers, voire des millions d'utilisateurs, il est difficile de vouloir négocier des avantages particuliers, le fournisseur ne pouvant pas avantager individuellement tel ou tel utilisateur. Il y a cependant des cas où le fournisseur définit plusieurs classes d'utilisateurs, plus ou moins avantagés selon leur abonnement.

3.5.3 Les aspects écologiques

Il est rassurant d'espérer que l'utilisation du *cloud* permettra de diminuer l'éparpillement de machines individuelles, qui souvent – dans le cas de petits serveurs – tournent « à vide » la plupart du temps.

Certains rapports mettent en avant le fait que les machines de dernière génération utilisées dans les centres de *cloud* bénéficient aussi d'un meilleur rendement énergétique[6].

Le gain écologique et énergétique constitue un argument de vente des acteurs du *cloud*, certains mettant en évidence des économies allant jusqu'à 90 % (sachant qu'en matière de publicité « jusqu'à » n'est jamais un engagement ferme (« *our system cuts power usage by up to 90 % compared to traditional systems*»[7]).

Cependant, pour constater une réelle différence globale, il faudrait pouvoir compter sur un net progrès du côté des périphériques (par exemple une généralisation des

[6] Expert Group Report for the European Commission – DG Information Society and Media (Lutz Schubert and al.) "The Future of Cloud Computing (Opportunities for European Cloud Computing beyond 2010)" p. 14.
[7] Amplidata sur Belgium Cloud http://www.belgiumcloud.com/?page_id=1956.

tablettes dépourvues de disque dur interne) car un PC ou un serveur utilisé comme périphérique en réseau ne consomme pas moins que la même installation indépendante. Or, on l'a vu, la plupart des entreprises qui ont recours au *cloud* sont contraintes d'adopter une solution hybride (le « tout *cloud* » n'est pas d'actualité). Les périphériques nouveaux ne remplacent pas, mais viennent en supplément des périphériques classiques.

Certains mettent donc en avant un revers de médaille écologique, sur base des arguments suivants[8] :

- Le cloud se compose de gros centres de traitement distants et interconnectés par des réseaux à grande bande passante, dont chaque composant est consommateur d'énergie ;
- Ces gros « data centers » sont fort énergivores et leur fonctionnement est soumis à des contraintes complémentaires (espace au sol, climatisation, refroidissement, ventilation, protection, éclairage de nuit, surveillance) ;
- Une grande part de l'énergie est quand même gaspillée et ne sert qu'à répondre aux pics de charge ;
- En plus de la consommation d'électricité, il est indispensable de doubler l'installation par des batteries et des groupes électrogènes qui permettent de garantir un fonctionnement en continu tout en comprenant (et émettant quand ils fonctionnent) une quantité importante de polluants ;
- Cette empreinte écologique s'ajoute aux empreintes précédentes, mais ne les remplace généralement pas.

Un des grands acteurs établis en Belgique (Google) adopte un ton fort différent, mais cela ne constitue pas un démenti et illustre l'exception que constitue ce site : « notre centre (de St. Ghislain près de Mons) est le premier au monde à fonctionner entièrement sans réfrigération, utilisant à la place un système basé sur l'évaporation des eaux industrielles d'un canal voisin. Cela aide nos ordinateurs à tourner avec une efficacité optimale et réduit la consommation globale d'énergie »[9].

[8] Isabelle Renard – Le cloud computing en France – 16 octobre 2012 (exposé).
[9] http://www.google.com/about/datacenters/locations/st-ghislain/.

Figure 2 - Google data centre (St. Ghislain, Belgique)

3.5.4 Les aspects économiques

Du point de vue du client

- **Réduction des coûts d'entrée**
  La réduction des coûts liés à l'acquisition et à la maintenance d'une infrastructure informatique est présentée comme le principal incitant pour les clients potentiels du *cloud*. Cette réduction (ou élimination) du ticket d'entrée est particulièrement intéressante pour les PME et entreprises naissantes, qui peuvent concentrer leurs capacités de financement sur le développement de leur cœur de métier et bénéficier directement des solutions informatiques les plus performantes sans devoir y investir leur capital.

- **Réduction du délai « pour être opérationnel »**
  Pour les mêmes raisons, spécialement pour les entreprises naissantes (startups et PME) l'effort pour être opérationnel et le délai (time to market) pour y parvenir est considérablement réduit. Cela permet d'être directement compétitif avec les entreprises établies de longue date. Pour les entreprises existantes, le *cloud* permet d'évoluer et de rester compétitif sans devoir consacrer trop de temps et de ressources à la gestion du changement.

- **Facturation selon l'usage**
  L'utilisation du *cloud* est un cas de passage de l'investissement en capital (CAPEX) à une dépense opérationnelle (OPEX).

- **Réduction du coût global (ou TCO)**
  Les fournisseurs de cloud mettent fortement en avant d'importantes économies globales (coût global de propriété ou « TCO ») liées à l'usage du *cloud* de préférence à une informatique traditionnelle : « *our system reduces TCO with up to 70 % compared to traditional systems*»[10]. Cette réduction espérée constitue évidemment un attrait majeur, principalement en temps de crise ou de réduction des budgets (publics et privés).

[10] Amplidata sur Belgium Cloud http://www.belgiumcloud.com/?page_id=1956

Dans certains exposés, les représentants de la Commission européenne et de certains gouvernements parlent même d'un potentiel d'économie (pour le secteur public passant au *cloud*) de près de 90 %[11]. Encore faut-il alors, dans la mesure où on ne met pas fin à la mission des agents de l'Etat concernés, pouvoir en réaffecter totalement le coût sur d'autres projets. La responsable du *cloud* public en Norvège (pays de 5 millions d'habitants) a cité une étude faite pour son gouvernement selon laquelle le passage au *cloud* générerait une économie annuelle de 825 millions d'euros[12]. Il est clair que le potentiel de réduction dépend du type de service (fonctionnalités, SLA, garanties) et de la faculté d'économiser totalement (ou de réaffecter à d'autres tâches) les dépenses liées à l'ancien système, notamment en ce qui concerne le coût des ressources humaines.

Du point de vue des acteurs du *cloud*

- **Un investissement important**
  La mise en place d'un *cloud* public par un « vendeur de ressources » exigera un investissement de départ plus important que s'il s'agissait d'une infrastructure privée : en effet, il faut être d'une part flexible pour s'adapter aux besoins très divers des clients et leur offrir une large interopérabilité, et d'autre part être extensible (« scalable ») afin de répondre à une charge d'utilisation variable en volume, sans limites prédéfinies. L'exigence de disponibilité permanente et la mise en place de mesures de sécurité et de redémarrage correspondantes augmentent l'investissement.

  Le montant de l'investissement varie fortement selon l'acteur concerné. Le fait d'attirer en Belgique un acteur majeur comme Google – qui y a établi un de ses trois plus grands centres de calcul européens se traduit selon cette entreprise par :
  - Un investissement d'un quart de milliard d'euro ;
  - 85 compagnies et sous-traitants actifs durant deux ans pour construire le centre (environ 2.000 emplois durant cette période) ;
  - 120 emplois permanents en période opérationnelle (pour assurer un fonctionnement de type 24x7).

- **Un système de facturation selon l'usage**
  L'adaptation des coûts à l'utilisation réelle des ressources nécessite la mise en place d'un support aux utilisateurs de qualité et d'un nouveau système de facturation lié aux indicateurs d'utilisation.

- **Un retour sur investissement « variable »**

[11] Exposé de Mr. Ken Ducatel, chef d'Unité « Software & services » – DG Connect - au symposium ECIS (European Committee for Interoperable Systems) « Bringing the cloud down to earth » du 24 avril 2013.
[12] Exposé de Mme Katarina de Brisis, Deputy Director General avec responsabilité pour le Cloud, - Ministry of Government Administration and Reform, Norway – symposium ECIS du 24 avril 2013.

Selon la plupart des analystes, ce point est critique pour beaucoup d'investisseurs et ne peut actuellement être garanti. Le retour sur investissement dépend du mode de financement (par les clients, par la publicité, mixte). Les ressources publicitaires étant directement liées à la masse des utilisateurs, cela peut se traduire pour les acteurs du *cloud* par une « course au client » en proposant au départ des conditions très attractives sans que la viabilité du système soit assurée. Il y aura inévitablement un moment où il faudra revoir ces conditions, ce qui peut placer le client dans une position très inconfortable : ou bien il part (comme il en a le droit) mais il risque dans ce cas de supporter des coûts élevés (à cause de la difficulté de migration des données vers un autre fournisseur qui n'aurait pas une offre absolument interopérable, d'absence de standards ouverts, de changement de processus), ou bien il reste en payant davantage.

3.5.5 Les rôles ou métiers du *cloud*

Le *cloud* permet aux acteurs (et personnes) d'exercer plusieurs métiers ou rôles qui s'attachent à une activité économique ou technique précise et sont générateurs d'emploi. Une part de ses emplois (principalement ceux qui sont nécessaires pour le fonctionnement du fournisseur, sa sécurité, son audit) peuvent se substituer à des emplois traditionnels de l'informatique d'entreprise ou de département, tout en étant facilement délocalisables (vu la mobilité des infrastructures *cloud*). C'est un point auquel il faut être attentif dans le souci de maintenir ou d'attirer cette activité en Belgique.

Le f**ournisseur** de *cloud* (*cloud* provider) est celui qui propose un service *cloud* aux clients, soit par des interfaces applicatifs dédiés (APIs ou plateformes PaaS), par l'offre de machines virtuelles (partagées) ou par l'offre d'accès direct, plus ou moins privé, à des ressources d'infrastructure (IaaS : puissance, stockage etc.) de plateforme ou d'applications. Les métiers sont en nombre et variés selon l'importance du centre, durant son érection (métiers spécialisés de la construction) et durant son fonctionnement (ingénieurs, administrateurs, opérateurs, agents de sécurité).

L'**intégrateur** de *cloud* (ou « revendeur ») est un acteur de service qui se charge d'implémenter de manière opérationnelle un service *cloud* auprès d'un client. Il peut se charger de créer pour le client une interface unique qui donne accès à divers types de *cloud* (par exemple au cas où un même client utilise des services différents pour la gestion de ses relations avec sa clientèle (le CRM), son courrier électronique, son archivage des données). Il assistera le client dans les choix qui correspondent le mieux à ses besoins. Il peut se charger de tâches de formation, gestion du changement etc.
L'intégrateur peut également être un **conseiller**, quoi que cette mission de consultance doive se faire de manière indépendante de toute revente. Ici aussi, il s'agira, spécialement lors d'études préalables ou d'audits, d'évaluer les services qui répondent le mieux aux besoins, sans négliger les perspectives économiques (à qui confier ses données, pour quel bénéfice), techniques (sous quels standards, niveau d'interopérabilité) et juridiques (sous quel régime contractuel et légal, dans quel écosystème européen ou non, et sous quelles garanties).

Cette analyse doit être poussée en fonction de la nature des activités de l'entreprise : le niveau de sécurité attendu pour les données, le degré de transparence du système, la performance et la disponibilité des services, l'adéquation des applications de l'entreprise au modèle de *cloud computing* et la gestion du risque de se voir « prisonnier de son fournisseur (vendor lock-in) ».
Utiliser un service *cloud* pour donner accès à des applications standards et conserver ses documents (les applications bureautique de Google par exemple) est simple, mais intégrer des services *cloud* à une informatique de production critique pour l'entreprise et en tirer de réels avantages l'est beaucoup moins.
Les entreprises qui migreront certaines de leurs applications vers le *cloud* auront besoin d'un conseiller compétent pour évaluer les contrats de niveau de service (SLAs) proposés par les fournisseurs. Alors qu'aujourd'hui les contrats protègent essentiellement le fournisseur, cette situation se modifiera rapidement sous la pression de la clientèle qui demandera des termes et conditions basés sur ses besoins et une gouvernance transparente du fournisseur.

L'expertise en matière de **sécurité et** l'**audit** constituent un métier en soi. Les clients les plus importants seront intransigeants sur la capacité de leur(s) fournisseur(s) à fournir la capacité et la performance nécessaire afin d'obtenir un haut niveau de satisfaction des utilisateurs tout en assurant la sécurité des données. Ils demanderont très certainement d'avoir la possibilité de surveiller et mesurer certains paramètres caractéristiques du fonctionnement du système global.

L'**éditeur de logiciels** applicatifs peut créer des produits pouvant fonctionner sur le *cloud* (ou adapter des produits existants) et placer ces produits auprès d'un fournisseur de *cloud*, pour que ce dernier les propose à ses clients et lui restitue une partie des redevances payées par les clients qui adopteront le service SaaS. C'est ainsi qu'un logiciel de gestion de clientèle ou de gestion de projets peut être installé par l'éditeur chez divers fournisseurs de *cloud*. Ce nouveau marché constitue pour les éditeurs une alternative à la vente pure et simple de licences au client final.

Dans ce cadre, il ne faut pas négliger l'activité d'adaptation ou de réécriture des applications. Un des intérêts du *cloud* est de permettre l'ajustement dynamique des ressources en fonction de la charge imposée aux applications ; cette possibilité est d'autant plus appréciable que la charge est variable. Les entreprises ont donc intérêt (tant du point de vue financier que de celui de la qualité des services offerts à ses employés, ses clients et ses fournisseurs) à migrer ce type d'applications de leur infrastructure interne, nécessairement surdimensionnée pour supporter les variations de charge, vers un service *cloud*. Cette stratégie ne sera cependant efficace que si les applications (en particulier leur architecture) sont adaptées aux caractéristiques de fonctionnement spécifiques du *cloud*. Il est donc également judicieux de concevoir les nouvelles applications dans cet esprit.

Il y a d'autres **fournisseurs d'outils** ou **composants** *cloud* (matériel ou logiciel) pour lesquels ce nouveau marché représente une opportunité économique : serveurs, dispositifs de stockage, infrastructure de réseaux de télécommunication, sécurisation, environnements de développements, programme de gestion de parc de machines virtuelles par répartition de charge, etc.

Ce qui est vrai pour les applications l'est également pour les infrastructures, dans la mesure où le modèle hybride est celui qui sera le plus adopté et où les entreprises continueront à concevoir et gérer leurs propres centres de calcul. En d'autres termes, les concepts et techniques sous-tendant le fonctionnement du *cloud* (la virtualisation et la réallocation dynamique des ressources par exemple) vont aussi se voir appliqués dans les centres de calculs privés. Il y a donc là aussi une expérience métier précieuse à valoriser.

Enfin au sein des **utilisateurs directs** ou « finaux », une série de compétences sont requises pour contracter (décider), contrôler, gérer les droits, former, évaluer l'impact économique de l'utilisation du *cloud*.

4 Opportunités et risques du *cloud computing*

4.1 Opportunités du cloud computing

Le *cloud* présente de nombreuses opportunités ou bénéfices, qui découlent des caractéristiques que nous venons d'évoquer :

- Il y a réduction du besoin de dépenses en capital liées à la création d'une infrastructure et/ou à l'acquisition de licences applicatives ;
- L'entreprise peut se concentrer, non sur son informatique, mais sur ses clients, sur l'efficacité de son personnel (utilisateur du *cloud*) et leurs besoins, c'est-à-dire son activité essentielle ;
- Les coûts deviennent opérationnels, et sont liés à la performance et à l'activité réelle de l'entreprise (pas d'activité = pas de coût ; grande activité génératrice de profits = coûts proportionnels) ;
- L'entreprise bénéficie de l'économie d'échelle liée au partage des ressources avec de nombreux autres utilisateurs (réduction des coûts unitaires) ;
- L'entreprise bénéficie de performances plus stables ou « lissées » réparties entre un grand nombre d'utilisateurs qui ne travaillent pas tous en même temps ;
- Les utilisateurs comprennent mieux le coût directement lié à leur activité (les charges peuvent être réparties dans l'entreprise en fonction de critères objectifs) ;
- La re-facturation de coût réel des services rendus aux clients de l'entreprise utilisatrice est facilitée et peut être justifiée ;
- Au meilleur contrôle des coûts (qui deviennent plus opérationnels) correspond une réduction des frais généraux et un meilleur contrôle des profits opérationnels (revenus – coûts opérationnels et FG) ;
- La gestion prévisionnelle des besoins est grandement facilitée : on ne doit plus se soucier de savoir comment prévoir, anticiper et absorber d'éventuels pics de charge ;
- L'entreprise est plus agile, plus flexible quant à l'essai, à la décision d'utiliser ou non, voire d'abandonner telle ou telle application. En conséquence, un nouveau service aux clients peut être lancé plus rapidement et à moindre risque ;
- L'entreprise est libérée de l'impératif de mettre périodiquement « à niveau » (upgrading) les infrastructures, les plateformes et les applications. Il n'est plus nécessaire de supporter ces coûts considérables et « à sens unique » : on paie à la demande et on peut revenir à la situation antérieure si la demande n'existe plus ;
- Le sentiment de sécurité n'est pas diminué. Il est plutôt augmenté, surtout dans le cas des PME et des utilisateurs individuels qui ne font pas de backup journalier de leurs données : quiconque a déjà vu son PC se faire voler ou son disque dur devenir illisible n'a pas besoin d'un long discours pour comprendre les avantages du *cloud* : e-mails, contacts, les documents et photos ne sont plus perdus. On les retrouve immédiatement sur le *cloud* avec un PC neuf.

Ces opportunités ou bénéfices existent tant dans le secteur public que dans le secteur privé. Il en résulte que pour la quasi-totalité des fournisseurs et pour un grand nombre des responsables informatiques, le *cloud computing* présente des avantages considérables avec en plus – pour les premiers – une opportunité de développer une nouvelle activité économique.

Dans ce cadre, les mises en garde des experts en sécurité, les objections formulées par les juristes quant à la protection des données et la nécessité de certitude quant au régime juridique de leur traitement ou conservation apparaissent souvent comme malvenues. Il faut cependant examiner les risques, comme le cadre juridique du *cloud* et les règles qui en découlent, non pour bloquer l'adoption du *cloud*, mais pour encadrer et rendre plus fiable l'ensemble de la branche d'activité.

4.2 Risques du cloud computing

4.2.1 Classification des risques

Il est avantageux de classifier les risques du *cloud computing* en fonction du modèle de service (IaaS, PaaS ou SaaS) et du modèle de déploiement (public, privé, hybride). En effet, cette classification permet de se concentrer sur les risques qui sont vraiment pertinents pour chaque situation.

4.2.1.1 Classification en fonction du modèle de service

L'entité qui fait appel à un fournisseur de services *cloud*, tout en restant propriétaire des actifs informatiques hébergés par le *cloud*, abandonne une partie du contrôle et de la visibilité sur les personnes, les processus et les techniques utilisées pour gérer ces actifs. Le niveau de visibilité est à considérer quand on identifie les risques et qu'on les évalue. En effet, chaque modèle de service *cloud* a sa propre visibilité qui varie en fonction du nombre de couches du modèle de services qui sont prises en charge par le *cloud*. Le modèle IaaS offre un fort niveau de visibilité à l'entité utilisatrice parce qu'il remplace uniquement l'infrastructure, alors que le modèle SaaS offre une plus faible visibilité parce qu'il remplace non seulement l'infrastructure, mais aussi les logiciels système, les données et les applications. Dans le modèle IaaS, l'entité utilisatrice de services *cloud* gère elle-même les risques liés à la gestion des logiciels système, des données et des applications, alors que dans le modèle SaaS, elle externalise cette gestion sur base de contrats de niveau de services (SLA – *Service Level Agreements*) avec son fournisseur.

Les risques liés à l'utilisation du *cloud* sont cumulatifs en fonction du modèle de service auquel ils se rattachent : le modèle IaaS présente une série de risques qui lui sont spécifiques et qui sont liés à la gestion de l'infrastructure ; le modèle PaaS présente les mêmes risques avec, en plus, ceux qui sont spécifiques à ce modèle et qui sont liés à la gestion des logiciels système ; enfin, le modèle SaaS présente, en plus, les risques spécifiques qui sont liés à la gestion des données et des applications.

4.2.1.2 Classification en fonction du modèle de déploiement

Certains risques sont spécifiques au modèle de déploiement du *cloud* : privé, public, ou hybride. Le facteur déterminant est le degré de confiance qui lie les participants (le fournisseur de services *cloud* et les entités utilisatrices du *cloud* ; les entités utilisatrices entre elles). En particulier, un *cloud* public est utilisé par des entités qui n'ont rien en commun et qui ne sont liées par aucun lien de confiance, alors que les entités utilisatrices d'un *cloud* privé peuvent en avoir. Les risques associés à l'utilisation du *cloud* sont différents dans ces deux cas.

4.2.1.3 Risques génériques

Il y a des risques liés à l'utilisation du *cloud* qui sont génériques, c'est-à-dire qu'ils ne dépendent ni du modèle de service, ni du modèle de déploiement.

4.2.2 Fiches de description des risques

Les risques sont présentés sous forme de fiches. Une fiche se présente comme suit :

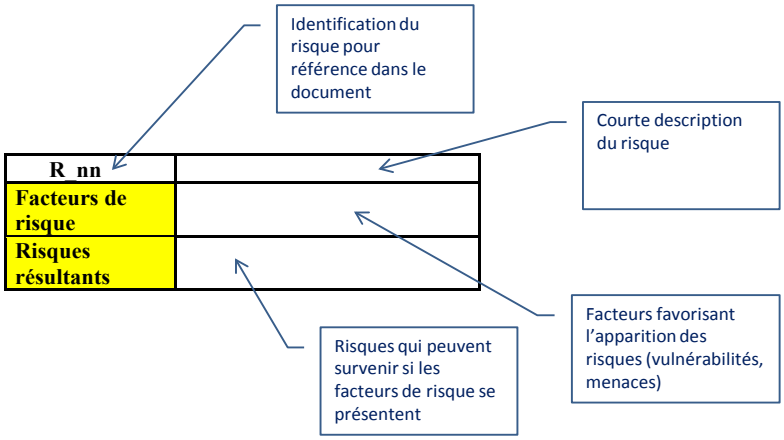

Figure 3 – Fiche de description de risque

4.2.2.1 Risques classifiés par modèle de service

4.2.2.1.1 IaaS

Risques spécifiques au modèle IaaS :

R_01	**Transfert hors des frontières (UE/EEE)**
Facteurs de risque	Les fournisseurs de service *cloud* sont souvent des multinationales, et l'information peut être localisée dans des pays dont la législation diffère de celle à laquelle l'entreprise est soumise, en particulier ce qui concerne la protection des données à caractère personnel. Les autorités du pays où l'information aboutit peuvent exiger l'accès à l'information, parfois sans garantie que l'accès est justifié.
Risques résultants	• Divulgation de données non autorisée • Non-conformité aux lois

R_02	**Multi-*tenancy***
Facteurs de risque	Pour profiter des avantages du *cloud*, une entité utilisatrice partage les ressources (espace de stockage, hardware, réseau…) avec les autres entités. Les ressources doivent être isolées pour éviter la divulgation d'une entité à l'autre. Des défauts d'isolation peuvent se produire, par exemple quand un espace de stockage est libéré par une entité, puis récupéré par une autre sans que le contenu soit effacé.
Risques résultants	• Divulgation de données non autorisée

R_03	**Contrôle des mesures de sécurité**
Facteurs de risque	Le fournisseur de services *cloud* doit s'équiper de protections et installer les politiques et processus associés afin d'atteindre au minimum le niveau de sécurité exigé par l'entité utilisatrice du *cloud*. L'entité utilisatrice n'a pas toujours la possibilité de vérifier que le fournisseur de services remplit ses obligations.
Risques résultants	• Blocage dû à l'indisponibilité du *cloud* • Perte d'information • Divulgation de données non autorisée

R_04	**Infrastructure délocalisée**
Facteurs de risque	La délocalisation (*offshoring*) de l'infrastructure augmente les sources possibles d'attaques. Le contrôle de la sécurité par le fournisseur de services *cloud* et la vérification par l'entité utilisatrice du *cloud* peuvent être difficiles dans des pays éloignés.
Risques résultants	• Blocage dû à l'indisponibilité du *cloud* • Perte d'information • Divulgation de données non autorisée

R_05	**Maintenance des machines virtuelles**
Facteurs de risque	Les fournisseurs de service IaaS permettent aux entités utilisatrices de créer des machines virtuelles suivant leurs besoins. Ces machines virtuelles doivent recevoir des correctifs (*patches*). Dans le cadre d'un service IaaS, c'est généralement la responsabilité de l'entité utilisatrice du *cloud*. Des machines virtuelles non utilisées peuvent être oubliées et laissées en l'état, ce qui laisse la porte ouverte aux attaques.
Risques résultants	• Blocage dû à l'indisponibilité du *cloud* • Perte d'information • Divulgation de données non autorisée

R_06	Authentification
Facteurs de risque	L'authentification doit être mutuelle entre le fournisseur de services *cloud* et l'entité utilisatrice du *cloud*. Alors que l'accent est souvent mis sur l'authentification de l'entité utilisatrice vis-à-vis du fournisseur de service, l'authentification dans l'autre sens peut être négligée, ce qui ouvre la voie à des usurpations d'identité ou à des attaques par intermédiaire (*man-in-the-middle attack*).
Risques résultants	• Divulgation de données non autorisée

4.2.2.1.2 PaaS

Risques spécifiques au modèle PaaS, qui s'ajoutent aux risques spécifiques au modèle IaaS :

R_07	Utilisation du SOA
Facteurs de risque	L'architecture SOA (*Service Oriented Architecture*), souvent présente dans l'offre PaaS, peut présenter des vulnérabilités, soit au sein des services eux-mêmes, soit au travers de leurs interactions. Les librairies SOA sont gérées par le fournisseur de services *cloud*, et l'entité utilisatrice n'a pas le contrôle direct sur la gestion de ces éléments, ce qui peut laisser la place à des vulnérabilités publiées mais non corrigées.
Risques résultants	• Blocage dû à l'indisponibilité du *cloud* • Perte d'information • Divulgation de données non autorisée

R_08	Fin de contrat
Facteurs de risque	En fin de contrat entre le fournisseur de services *cloud* et l'entité utilisatrice, les applications qui ont été développées dans l'environnement PaaS doivent être effacées du *cloud* par le fournisseur de service. Si des détails échappent à la procédure d'effacement et subsistent sur le *cloud*, ils peuvent être récupérés par un tiers et révéler des vulnérabilités de l'application.
Risques résultants	• Perte d'information • Divulgation de données non autorisée

4.2.2.1.3 SaaS

Risques spécifiques au modèle SaaS, qui s'ajoutent aux risques spécifiques aux modèles IaaS et PaaS :

R_09	Propriété des données
Facteurs de risque	Le fournisseur de services *cloud* fournit les applications, et l'entité utilisatrice apporte les données. Si la propriété des données n'est pas clairement définie, le fournisseur de services peut refuser l'accès aux données, voire exiger des frais supplémentaires en fin de contrat pour les restituer.
Risques résultants	• Perte d'information • Risque financier

R_10	Fin de contrat
Facteurs de risque	En fin de contrat entre le fournisseur de services *cloud* et l'entité utilisatrice, les données qui ont été stockées dans l'environnement SaaS doivent être effacées du *cloud* par le fournisseur de service. Si des données échappent à la procédure d'effacement et subsistent sur le *cloud*, elles peuvent être révélées à un tiers non autorisé.
Risques résultants	• Divulgation de données non autorisée

R_11	Cycle de développement des applications
Facteurs de risque	Le cycle de développement des applications (SDLC – *System Development Life Cycle*) est sous le contrôle du fournisseur de services *cloud*. L'entité utilisatrice a peu de contrôle, en particulier sur les exigences de sécurité qui ont été prises en compte au long du cycle de développement. Ce manque de contrôle peut aboutir à un niveau de sécurité qui ne remplit pas les besoins des utilisateurs de l'application.
Risques résultants	• Blocage dû à l'indisponibilité des applications sur le *cloud* • Perte d'information • Divulgation de données non autorisée

R_12	Gestion des identités et des accès
Facteurs de risque	Les fournisseurs de services *cloud* offrent leurs services et leurs applications à plusieurs entités en même temps, ce qui exige une gestion des identités et des accès (IAM – *Identity and Access Management*). Si le fournisseur de services *cloud* ne gère pas l'IAM correctement, les applications et – au travers des applications – les données qu'elles traitent peuvent être lues ou modifiées par d'autres entités utilisatrices du *cloud*.
Risques résultants	• Divulgation de données non autorisée • Perte d'information

R_13	Changement de fournisseur
Facteurs de risque	Rien n'est généralement prévu pour faciliter la portabilité du service et des données d'un fournisseur de services *cloud* à un autre, en particulier quand le fournisseur ne rend pas un service satisfaisant ou qu'il tombe en faillite, ou que (pour éviter la faillite) il révise ses conditions contractuelles. De même, la décision d'une entité utilisatrice du *cloud* de renoncer à ce service et de rapatrier les services et les données en interne se heurte à des difficultés.
Risques résultants	• Blocage dû à l'indisponibilité des applications sur le *cloud* • Blocage dû à l'indisponibilité des données sur le *cloud* • Perte d'information

R_14	Conformité aux politiques d'achat
Facteurs de risque	Les politiques d'achat de matériel et de logiciel des entreprises peuvent être négligées quand l'entreprise opte pour un service *cloud*, ce qui peut mener à des incompatibilités entre les applications du *cloud* et les applications qui sont exploitées en interne.
Risques résultants	• Blocage dû à des dysfonctionnements des applications sur le *cloud*

R_15	Vulnérabilité des navigateurs internet
Facteurs de risque	Les applications offertes par les fournisseurs SaaS sont généralement accessibles au travers d'un navigateur (*browser*) et d'une connexion sécurisée. Les navigateurs sont une cible courante d'attaques. Si le navigateur est compromis, l'application l'est aussi ; la connexion sécurisée ne résout pas le problème.
Risques résultants	• Blocage dû à l'indisponibilité des applications sur le *cloud* • Perte d'information • Divulgation de données non autorisée

4.2.2.2 Risques classifiés par modèle de déploiement

4.2.2.2.1 Cloud public

R_16	Partage avec de nombreuses entités
Facteurs de risque	Le *cloud* public est partagé entre de nombreuses entités utilisatrices qui n'ont pas d'intérêt commun ni d'exigence identique en matière de sécurité. Les opportunités de violation de la sécurité sont plus nombreuses.
Risques résultants	• Blocage dû à l'indisponibilité des applications sur le *cloud* • Perte d'information • Divulgation de données non autorisée

R_17	Dommages collatéraux
Facteurs de risque	Une attaque vers une entité utilisatrice d'un *cloud* public peut avoir un impact sur les autres entités utilisatrices du même *cloud*. C'est particulièrement le cas des attaques distribuées par déni de service (DDoS – *Distributed Denial of Service*), ainsi que de l'exploitation des vulnérabilités du logiciel géré par le fournisseur de services *cloud*, que le fournisseur tarde parfois à corriger.
Risques résultants	• Blocage dû à l'indisponibilité des applications sur le *cloud* • Perte d'information • Divulgation de données non autorisée

4.2.2.2.2 Cloud privé

R_18	Investissements nécessaires
Facteurs de risque	Un *cloud* privé peut être perçu par une entreprise comme un moyen de supprimer les coûts liés à l'acquisition, à la maintenance et aux opérations des systèmes informatiques. Il est parfois difficile de faire accepter par les gestionnaires de l'entreprise qu'il y a un coût lié à l'adoption d'un *cloud* privé ; les budgets sont parfois rognés, ce qui mène à des capacités insuffisantes.
Risques résultants	• Risque financier ; coûts imprévus • Blocage dû à l'indisponibilité des applications sur le *cloud*

4.2.2.2.3 Cloud hybride

Les risques sur le *cloud* hybride sont la combinaison des risques sur les *clouds* privé et public. De plus, le risque suivant est spécifique au *cloud* hybride :

R_19	Interdépendance
Facteurs de risque	Dans le cas où différents types de *cloud* sont mélangés, un *cloud* d'un type peut avoir besoin d'accéder à un *cloud* d'un autre type. Si les niveaux de sécurité sont différents, cela peut mener à la nécessité d'accéder à des systèmes dont la sécurité est critique à partir de systèmes moins critiques. Les mesures spéciales de sécurité qui sont nécessaires ne sont pas toujours mises en place.
Risques résultants	• Perte d'information • Divulgation de données non autorisée

4.2.2.3 Risques génériques

Le risque suivant ne dépend ni du modèle de service, ni du modèle de déploiement :

R_20	Coût
Facteurs de risque	Une entité utilisatrice de services *cloud* peut voir ses systèmes hébergés sur le *cloud* bloqués par le fournisseur de services s'il ne paye pas les redevances à temps à son fournisseur.
Risques résultants	• Risque financier • Blocage dû à l'indisponibilité des applications sur le *cloud*

4.3 Gestion des risques

Une fois les risques identifiés (voir §4.2), il convient de les gérer et de déterminer quelles mesures de sécurité réduisent ces risques jusqu'à un niveau acceptable par l'entreprise, et ce, de la manière la plus économique possible.
L'approche proposée ici comporte quatre étapes :

1. Evaluation des risques – Les risques qui ont été identifiés et qui sont liés à l'introduction du *cloud* doivent être évalués afin de déterminer ceux qui doivent être réduits et qui doivent être couverts en priorité ;
2. Revue des politiques – Afin de se préparer à l'introduction du *cloud* dans l'entreprise, les politiques de sécurité doivent être revues (et, dans certains cas, créées). Cette étape assure que les règles de sécurité sont bien établies ;
3. Traitement des risques – Dans cette étape, on détermine les mesures de sécurité qui sont nécessaires pour couvrir de manière appropriée les risques prioritaires ; on sélectionne le fournisseur de services *cloud* en lui imposant ces mesures ;
4. Usage contrôlé du *cloud* – On utilise les services du fournisseur de service *cloud* tout en maintenant la surveillance de ses prestations, particulièrement en matière de sécurité.

Les étapes sont illustrées ci-dessous :

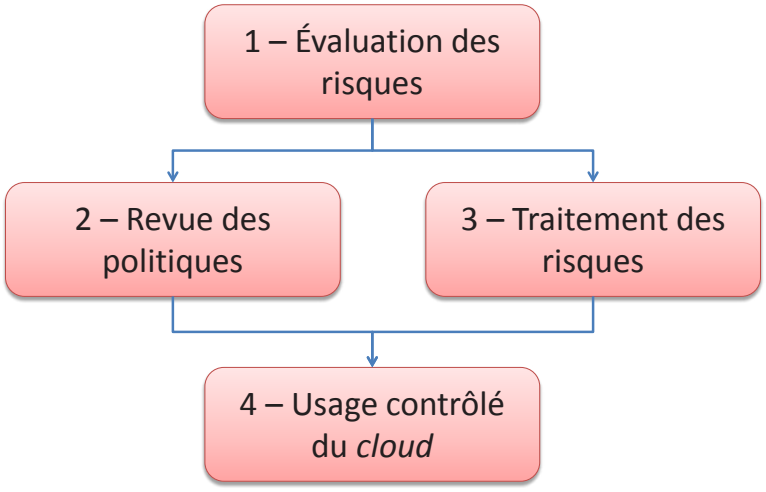

Figure 4 – Gestion des risques

4.3.1 Evaluation des risques

Deux méthodes existent pour réduire les risques jusqu'à un niveau qui est acceptable :

- Agir sur la source – On s'efforce de diminuer la probabilité qu'une menace s'exerce sur l'informatique et les informations ;
- Agir sur la cible – On met en place des mesures de sécurité plus strictes qui protègent mieux les informations contre les vulnérabilités du système informatique.

On le voit, le but n'est pas d'éliminer le risque (on ne peut jamais l'éliminer entièrement), le but est de le diminuer jusqu'à un niveau résiduel qui est considéré comme acceptable par l'entreprise. C'est la direction de l'entreprise qui peut décider si un risque résiduel est acceptable ou non, pas le service informatique. Néanmoins, la direction a besoin de l'avis de ses informaticiens pour prendre des décisions en connaissance de cause.
Afin de pouvoir décider si un risque peut être accepté, il faut l'évaluer. Même s'il est impossible d'évaluer un risque de manière tout à fait rigoureuse (un risque est par nature inconnu), des méthodes structurées permettent une évaluation pratique et des comparaisons. Un exemple de méthode très simple à mettre en œuvre consiste à évaluer les risques sur base de deux facteurs : la probabilité d'occurrence de la menace d'une part, et les vulnérabilités que la menace tentera d'exploiter d'autre part. On place les risques sur une échelle bidimensionnelle comme ci-dessous :

Menace / Vulnérabilité	Probabilité d'occurrence faible (exemple : 1 fois par an)	Probabilité d'occurrence moyenne (exemple : 1 fois par mois)	Probabilité d'occurrence forte (exemple : 1 fois par jour)
Vulnérabilité importante (une technique peu élaborée permet de menacer la sécurité)			
Vulnérabilité normale (il faut une expertise particulière pour menacer la sécurité)			
Vulnérabilité faible (il faut des efforts démesurés pour menacer la sécurité)			

Tableau 1 – Echelle d'évaluation des risques

On place chaque risque identifié sur l'échelle en fonction d'une estimation de la probabilité d'occurrence de la menace (axe horizontal) et de la vulnérabilité des systèmes informatiques que la menace peut exploiter (axe vertical).

4.3.2 Revue des politiques

Les politiques de sécurité de l'entreprise doivent être revues (voire créées si elles n'existent pas encore) avant toute utilisation d'une nouvelle solution informatique. Ce principe s'applique au *cloud* comme à toute nouvelle solution. Les domaines suivants peuvent faire l'objet de la revue :

- Classification de l'information – Afin de garantir un niveau de protection approprié aux informations, il convient de les classifier pour indiquer le degré souhaité de protection lors de leur manipulation. Certaines informations peuvent nécessiter un niveau de protection spécial parce que leur perte ou leur divulgation met l'entreprise en danger ;
- Conformité aux exigences légales – L'entreprise est soumise aux lois de protection des informations à caractère personnel, et la politique de sécurité de l'entreprise doit refléter les obligations en cette matière. Certains secteurs, comme la santé ou les institutions financières, sont soumis à des exigences légales spécifiques qui se reflètent aussi dans leurs politiques de sécurité ;
- Continuité des opérations – Si l'entreprise a une politique en matière de reprise après désastre, celle-ci se matérialise par un plan de continuité (*Business Continuity Plan*) ;
- Politique d'achat de matériel et de logiciel – Le cas échéant, l'entreprise doit s'assurer qu'il n'y a pas d'incompatibilité entre les applications offertes sur le *cloud* et celles qu'elle continue à exploiter en interne.

La revue de ces domaines avant l'introduction du *cloud* peut mener à des modifications :

- Classification de l'information – L'entreprise peut décider de créer une classe d'informations particulièrement sensibles qui ne seront jamais transférées sur un *cloud* si le risque de perte ou de divulgation est évalué comme trop élevé dès lors qu'on les migre sur un *cloud*. Ceci pourrait s'appliquer à des descriptions de procédés industriels ou de stratégie commerciale, dont la divulgation à des tiers pourrait mettre la pérennité de l'entreprise en péril ;
- Conformité aux exigences légales – L'entreprise peut décider de créer une classe d'informations à caractère personnel qui ne seront jamais transférées sur un *cloud* si le risque d'utilisation non contrôlée est évalué comme trop élevé dès lors qu'on les migre sur un *cloud*. Par exemple, dans un hôpital, les données médicales des patients peuvent faire l'objet d'une telle classification ;
- Continuité des opérations – Quoique l'introduction du *cloud* n'ait un impact que sur le plan de continuité et, généralement, aucun impact sur la politique de continuité, il est prudent de revoir cette politique à la lumière des nouveaux risques liés à l'utilisation du *cloud*. Si l'entreprise n'a pas encore de politique de continuité, l'introduction du *cloud* est l'occasion d'en établir une ;
- Politique d'achat – Elle doit éventuellement être revue si des applications sont utilisées en interne après l'introduction du *cloud*.

4.3.3 Traitement des risques

Une fois qu'on a évalué les risques sur l'échelle d'évaluation (voir l'exemple au point 4.3.1), on détermine quels sont les risques qui doivent être réduits et par quelles mesures.
Dans notre exemple, un risque qui, après évaluation, est placé sur une cellule verte est faible et peut ne pas être réduit ; un risque sur une cellule jaune est significatif et doit être réduit si possible ; un risque sur une cellule rouge est non acceptable et doit impérativement être réduit :

- Soit on diminue la probabilité par des mesures préventives. Par exemple, on fait la distinction entre les informations très sensibles (qu'on ne stocke jamais sur un *cloud*), et les autres informations (qui peuvent être stockées sur un *cloud*), et ce, afin de diminuer la probabilité de divulgation d'informations sensibles à l'extérieur de l'entreprise ;
- Soit on réduit les vulnérabilités par des mesures généralement techniques. Par exemple, on impose au fournisseur de services *cloud* de chiffrer toutes les informations — tant sur les réseaux que sur les unités de stockage, avec de la cryptographie forte.

Une fois qu'on a éliminé les risques « rouges » et qu'on a réduit les risques « jaunes » chaque fois que c'est possible, on obtient un ensemble de mesures de sécurité qui couvrent les risques de manière adaptée et qui réalisent le niveau de sécurité que l'entreprise veut atteindre.
La liste ci-dessous donne des exemples de mesures de sécurité à envisager (et à sélectionner suite à l'étape de traitement des risques) :

- Mesures contractuelles – L'entreprise peut imposer des clauses contractuelles au fournisseur de services *cloud* pour diminuer certains risques :
  - S'assurer que le contrat avec le fournisseur de services *cloud* garantit que l'entreprise utilisatrice reste l'unique propriétaire des informations et des applications qui ont migré sur le *cloud* ;
  - Ajouter au SLA du fournisseur de service *cloud* l'obligation d'avoir un processus de gestion de vulnérabilités des hyperviseurs[13] ;
  - Ajouter au SLA du fournisseur de service *cloud* l'obligation d'avoir un processus de gestion des changements qui inclut au minimum une analyse de risques ;
  - S'assurer que des dispositions existent qui permettent de changer de fournisseur de services *cloud* sans perdre des informations ou des applications et ce, dans des délais raisonnables ;
  - Si nécessaire, inclure des limitations géographiques pour la localisation de l'information qui réside sur le *cloud* ;

[13] En informatique, un **hyperviseur** (ou virtual machine monitor - VMM) est un composant logiciel ou matériel qui permet à un serveur « hôte » de gérer une ou plusieurs machines virtuelles (chacune de ses machines étant utilisée par exemple par un client du cloud).

- Mesures de sécurité mises en œuvre par le fournisseur – L'entreprise peut exiger des informations du fournisseur de service *cloud* :
  - Description des règles régissant qui, parmi le personnel du fournisseur de services *cloud* (ou de ses sous-traitants), a le droit d'accès aux informations de l'entreprise ;
  - Description des protections réseaux (pare-feu, antivirus, protection contre les attaques par déni de service…) mises en place par le fournisseur de services *cloud* ; description du processus de gestion de ces protections ;
  - Description du processus de gestion des droits d'accès au sein de l'organisation du fournisseur de services *cloud* ;
  - Description des mesures cryptographiques : algorithmes, longueur de clefs, gestion des clefs ;
  - Description des mesures techniques d'effacement de données libérées et de destruction de médias informatiques ;
  - Description du plan de continuité mis en place par le fournisseur de services *cloud* ; preuve que des exercices sont effectués régulièrement ;
  - Preuve que le fournisseur de services *cloud* fait l'objet d'audits réalisés régulièrement par des auditeurs certifiés ;
- Choix d'un mode particulier de gestion du *cloud* – L'entreprise peut décider de se limiter à un *cloud* privé si le caractère « *multi-tenant* » des *clouds* publics présente des risques évalués comme inacceptables ;
- Mesures mises en œuvre au sein de l'entreprise utilisatrice du *cloud* :
  - Organiser une campagne de sensibilisation à la sécurité de l'utilisation du *cloud* ;
  - Accéder au *cloud* exclusivement au travers de navigateurs sécurisés (utilisation de *sandboxes*) ou de stations virtuelles sécurisées ;
  - Revoir les plans de continuité (*Business Continuity Plan*, *Disaster Recovery Plan*) afin de parer à une indisponibilité prolongée du *cloud*.

4.3.4 Usage contrôlé du *cloud*

La sécurité est un processus continu, c'est-à-dire qu'elle ne s'arrête pas à l'établissement d'un service comme le *cloud* ; elle doit s'exercer aussi pendant l'exploitation du service.
L'entreprise utilisatrice de services *cloud* doit vérifier régulièrement que le fournisseur de services *cloud* remplit ses obligations contractuelles et, s'il le faut, obtenir des preuves ; il en va de même en ce qui concerne les mesures de sécurité mises en œuvre par le fournisseur de services.

D'autre part, l'entreprise doit vérifier que le programme d'audit IT auquel elle est soumise prend en compte l'utilisation du *cloud* et que ses auditeurs internes sont formés à ces vérifications.

5 Le marché du *cloud computing*

5.1 Situation actuelle en Europe et en Belgique

5.1.1 Le marché actuel du *cloud* en Europe

Selon une étude réalisée par IDC[14] pour la Commission européenne (DG Information Society) en juin 2012, le marché européen du *cloud* public pour 2011 représenterait un chiffre d'affaires de 4,6 milliards d'euros et de 6,2 milliards d'euros pour 2012. Ces chiffres correspondent respectivement à 1,6 % et 2,2 % des dépenses informatiques globales hors services.

Les services hardware représenteraient 1,1 milliard d'euros en 2011 et 1,5 milliard d'euros en 2012 tandis que les services software représenteraient respectivement 3,5 et 4,7 milliards d'euros.

Ces chiffres sont compatibles avec l'estimation du marché français effectuée par Markess au début de 2012 dont le volume global serait de 2,8 milliards d'euros, sachant que les *cloud*s privés et communautaires sont également repris dans ce chiffre.

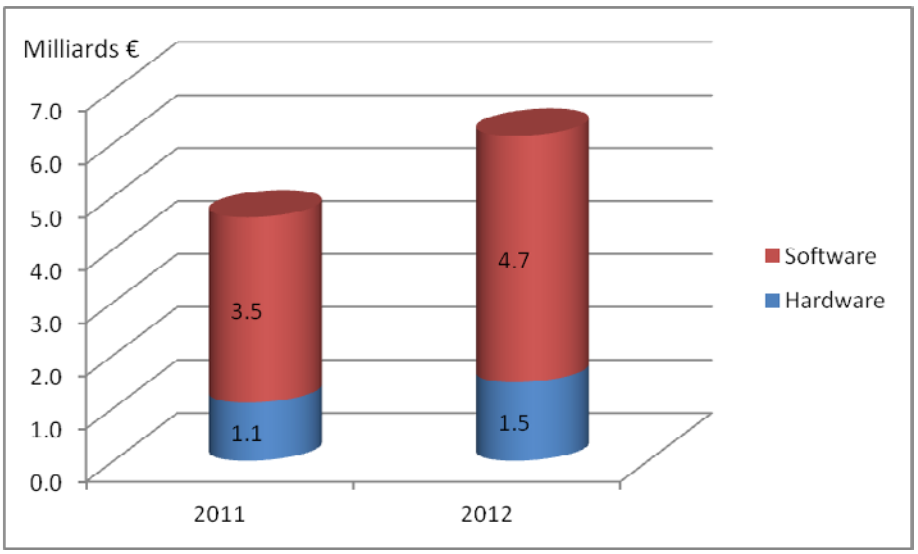

Figure 5 - Le marché actuel du cloud en Europe

Nous n'avons pas trouvé de chiffres relatifs au *cloud* en Belgique ; nous avons dès lors adopté l'hypothèse selon laquelle la part de la Belgique serait de 2,7 % (rapport du PIB belge au PIB européen).

[14] Quantitative Estimates of the Demand for Cloud Computing in Europe and the Likely Barriers to Up-take - IDC - Juin 2012.

Le tableau suivant représente les dépenses en technologie de l'information en Europe en 2009[15]. Sur cette base, la part de la Belgique serait de 2,6 % du marché européen de l'IT.

	IT Expenditure (bn$) - 2009
Germany	181
UK	153
France	136
Italy	104
Spain	73
Netherlands	49
Poland	26
Sweden	25
Belgium	24
Austria	21
Denmark	16
Finland	15
Greece	15
Czech Republic	15
Portugal	13
Ireland	12
Hungary	11
Romania	9
Slovakia	6
Bulgaria	3
Slovenia	2
Others	15
Total	**924**
Belgium %	**2.6%**

Figure 6 - Les dépenses en IT en Europe

En prenant une hypothèse conservatrice à 2,5 %, le chiffre d'affaires généré par les activités *cloud* en Belgique serait approximativement de 153 millions d'euros en 2012. Ce chiffre a été discuté avec les acteurs concernés lors de la réunion du 27 février 2013. Il appert cependant que le secteur ne semble pas avoir une vision consolidée des chiffres d'affaires générés.

[15] World Information Technology and Services Alliance – Digital Planet 2009.

5.1.2 Freins au développement du *cloud*

Les utilisateurs potentiels de services *cloud* sont confrontés à diverses barrières qui en ralentissent l'adoption. Les conclusions qui suivent résultent de l'étude IDC déjà citée ainsi que de celle réalisée par l'Expert Group de la DG Information Society and Media[16]. D'une manière générale, les freins repris ci-dessous sont unanimement reconnus et font l'objet de nombreuses publications sur internet :

- Une incertitude ou, à tout le moins, un manque de clarté, quant au respect des législations relatives à la protection et confidentialité des données personnelles (en particulier le cas du Patriot Act américain qui permettrait à la CIA ou au FBI d'accéder à des données gérées ou stockées sur le *cloud* par les entreprises établies aux USA sans que ces entreprises puissent prévenir le possesseur de celles-ci, en violation des lois européennes ou locales) ;
- Une incertitude ou, à tout le moins, un manque de clarté, quant à la loi applicable à des données qui, par définition, peuvent être stockées n'importe où dans le monde ;
- Certaines lois locales qui ne favorisent pas l'emploi du *cloud*, tel les incitants fiscaux qui favoriseraient les investissements en capital par rapport aux dépenses opérationnelles ;
- Le doute quant au fait que les données supprimées sont effectivement effacées définitivement des systèmes ;
- L'absence de principes, à minima harmonisés au niveau européen, relatifs à la responsabilité (et la réparation des dommages qui en découle) des fournisseurs de services *cloud* lors de la perte, destruction ou vol de données ;
- Le peu d'informations disponibles auprès des fournisseurs quant à la faisabilité et au coût du transfert de données d'un fournisseur à l'autre ;
- Le risque de voir les données confiées au fournisseur devenir dépendantes d'une architecture ou de standards propriétaires, qui rendent beaucoup plus difficile le transfert (*vendor locking*) ;
- Le manque de confiance quant à la capacité des fournisseurs d'assurer les services 24x7 avec le niveau de performance requis et la crainte de l'influence des indisponibilités des services sur le business ;
- L'absence, l'imprécision ou le caractère non contraignant des SLA proposés ;
- Dans certaines régions, le manque de bande passante des infrastructures de télécommunication ;
- Dans certaines régions, le coût trop élevé de l'accès à internet ;
- Le fait qu'il n'est pas assuré que le coût de l'utilisation de services *cloud* est substantiellement inférieur à celui de l'utilisation d'un système interne ;
- Le fait qu'il n'est pas assuré que les conditions et le prix fixés pour l'utilisation de service *cloud* soient pérennes : ne s'agit-il pas de « prix de lancement » ? - Peut-on s'attendre, comme c'est le cas actuellement pour les services bancaires, à des modifications unilatérales des conditions ?
- L'absence de software adéquat (en particulier proposés dans différentes langues) ;
- L'absence de support local ;

[16] The Future of Cloud Computing – European Commission / DG Information Society and Media – 2010.

- L'impossibilité de contrôler les changements de versions des logiciels mis à disposition et donc de risquer de se voir imposer des coûts de migration non désirés ;
- etc.

5.2 Evolution du marché du cloud computing en Europe et en Belgique

5.2.1 Les scénarios possibles

L'évolution du marché du *cloud* sera conditionnée par la disparition ou la diminution de l'importance de ces barrières techniques, fonctionnelles, économiques et juridiques décrites précédemment. Les études démontrent en outre que les raisons juridiques sont prédominantes : la certitude que les données supprimées sont effectivement effacées des systèmes, la protection de la confidentialité des données ainsi que la loi applicable aux données.

Les scénarios possibles sont donc :

- Le scénario pessimiste
  Un ralentissement de l'adoption du *cloud* après 2014 suite à l'absence d'intervention des autorités publiques pour encadrer le marché et à divers incidents relatifs à la sécurité, la confidentialité et la disponibilité des données ;
- Le scénario linéaire
  Une évolution linéaire de l'adoption du *cloud* en l'absence d'intervention des autorités publiques, sans incidents majeurs et avec une amélioration substantielle de la bande passante des infrastructures de télécommunication ;
- Le scénario optimiste / interventionniste
  Une accélération de l'adoption du *cloud* dès que les autorités publiques ont pris des mesures juridiques adéquates, en 2014/2015.

Les trois scénarios supposent cependant tous que :

- L'Europe sort de crise progressivement sans choc particulier ;
- Tous les paramètres macro-économiques progressent lentement ;
- La situation politique mondiale ne connaît pas d'évènement ayant une influence notable sur la structure politique ou l'économie européenne.

5.2.2 Le scénario pessimiste

Ce scénario résulte du fait que les incidents supposés détourneront définitivement les administrations publiques de l'utilisation du *cloud* et que son adoption par les entreprises se fera pour des applications limitées qui manipulent des données peu sensibles. Dans ce cas, l'utilisation du *cloud* gratuit (Gmail, Google apps, …) réduira le développement de solutions payantes à plus haute valeur.

Le taux de croissance actuel passerait de 33 % à 22 % en 2014.

Ce scénario conduit à une prévision de dépenses dans le *cloud* de 35,2 milliards d'euros à l'horizon 2020, soit 10,7 % des dépenses globales en technologies de l'information par rapport aux 2,2 % en 2012 ; l'évolution des dépenses globales en IT étant supposée linéaire avec un taux de croissance annuel moyen de 1,9 %.

Pour la Belgique, cela représenterait 880 millions d'euros en 2020.

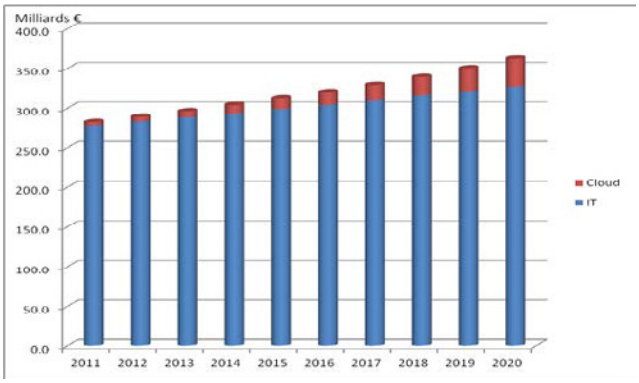

Figure 7 - Evolution du marché du cloud en Europe – Scénario pessimiste

5.2.3 Le scénario linéaire

Ce scénario résulte de l'absence d'incidents majeurs. Les administrations publiques restent réticentes du fait de l'absence de cadre juridique et réglementaire et développent des solutions communautaires ou « souveraines » (c'est déjà le cas en France et en Grande-Bretagne). L'adoption du *cloud* par les entreprises s'étendra à plus d'applications, pour autant qu'elles ne manipulent pas de données personnelles.

Le taux de croissance reste au niveau du taux actuel de 33 %.

Ce scénario conduit à une prévision de dépenses dans le *cloud* public de 59,9 milliards d'euros à l'horizon 2020, soit 18,7 % des dépenses globales en technologies de l'information par rapport aux 2,2 % en 2012 ; du fait du remplacement modéré des services internes par des services *cloud*, le taux de croissance annuel moyen des dépenses globales en IT se réduirait à 1,5 %.

Pour la Belgique, cela représenterait 1,5 milliard d'euros en 2020.

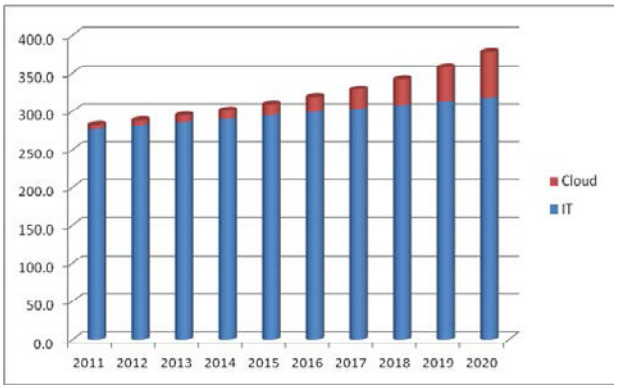

Figure 8 - Evolution du marché du cloud en Europe – Scénario linéaire

5.2.4 Le scénario optimiste / interventionniste

Il s'agit à proprement parler d'un scénario volontariste dans lequel les autorités publiques européennes et locales adoptent des mesures juridiques et réglementaires fortes pour annihiler les effets des freins correspondants.

Ces mesures devraient consister principalement à :

- Etablir des règles claires relatives aux responsabilités des fournisseurs en matière de sécurité et de confidentialité des données, quelle que soit leur localisation ;
- Etablir des règles claires relatives à la loi applicable aux données, quelle que soit leur localisation ;
- Harmoniser les règles relatives à la protection des données personnelles ;
- Instaurer une réglementation garantissant la portabilité des données entre fournisseurs ainsi que l'effacement complet et définitif des données supprimées par l'utilisateur ;
- Préciser les droits des utilisateurs de services *cloud*, notamment le traitement des plaintes et l'accès aux données (visualiser, modifier, supprimer).

Idéalement, l'application de ces mesures par les fournisseurs devrait pouvoir être contrôlée régulièrement par un organe public et donner lieu à des certifications locales ou européennes ; par exemple :

- Une certification Sécurité attestant que toutes les mesures garantissant la sécurité et la confidentialité des données ainsi que la protection des données personnelles sont prises et vérifiées régulièrement par des audits internes ;
- Une certification Services publics attestant que les services *cloud* sont conformes aux prescrits réglementaires des administrations publiques, avec éventuellement des restrictions relatives à la localisation des données (confinement local ou EU des données).

Ce scénario suppose également une amélioration notable de la bande passante des infrastructures de télécommunication et une réduction sensible des tarifs des fournisseurs d'accès à internet.

Dans ces conditions, le taux de croissance du chiffre d'affaires relatif aux services *cloud* s'accélèrera après 2014/2015 lorsque les mesures réglementaires auront été mises en place et passera de 33 % à 40 %. Par contre, la croissance des dépenses en informatique classique diminuera après 2014 du fait de la substitution massive de certains services internes par des services *cloud*, passant de 1,9 % à 1 %. La part des services *cloud* représentera 26 % des dépenses totales en technologies de l'information en 2020, soit 2 milliards d'euros pour la Belgique.

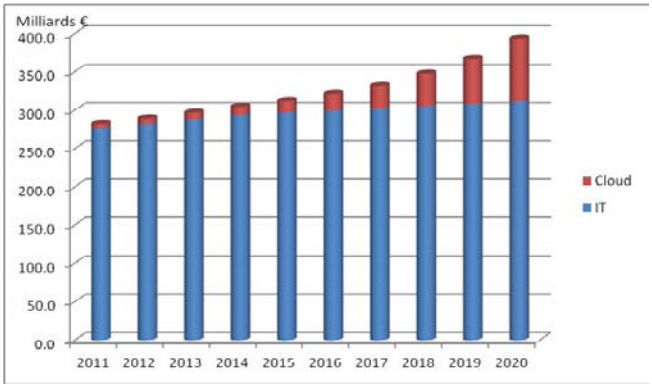

Figure 9 - Evolution du marché du cloud en Europe – Scénario optimiste

5.2.5 Opportunité d'une intervention directe de l'Etat ?

Le *cloud* souverain tel qu'il se met en place actuellement dans un Etat membre est-il nécessaire, souhaitable et/ou viable ?

Il s'agit de susciter, par des appels à projets généreusement subsidiés, la formation de consortiums destinés à aboutir à la création d'entreprises qui sont des partenariats public-privé (où l'Etat est actionnaire et exerce un pouvoir de contrôle).

Le but avoué est de maintenir localement (dans l'Etat membre en question, dans ce cas) l'ensemble de l'écosystème : les actionnaires, les centres de décision, l'infrastructure, la plateforme applicative et surtout les données. Il peut aussi être intéressant de contrôler les conditions contractuelles, notamment les prix[17].

Sans la promesse de subsides, les dits consortiums ou sociétés n'auraient sans doute pas vu le jour. Outre le caractère nécessairement politique de l'opération et les problèmes juridiques de distorsion de concurrence que cela peut entraîner dans un marché naissant ou qui existe déjà, ne va-t-on pas fabriquer artificiellement des entreprises opportunistes mais fragiles à terme qui ne pèseront pas lourd face aux vrais géants du marché – les Amazon, Google, Microsoft, IBM etc. –, et qui risquent d'être rachetées à vil prix par ces géants dès qu'elles auront épuisé leurs subsides et que l'Etat ne pourra plus continuer à les financer ?

[17] La présence de l'Etat peut servir à contrôler les prix (ce qui n'est cependant pas facile dans les secteurs où l'Etat est présent, comme l'électricité ou le gaz). C'est toutefois l'argument d'IBM (France) pour s'opposer à la présence de l'Etat dans la fourniture cloud.
(http://archives.lesechos.fr/archives/2012/lesechos.fr/01/31/0201873061845.htm.).

« Créer les conditions d'un fonctionnement compétitif, durable et équilibré du marché des biens et services en Belgique. »

A-t-on besoin de créer ainsi de nouveaux acteurs, alors que les grands spécialistes internationaux du *cloud* signent par ailleurs des accords avec des partenaires locaux pour développer ces offres de *cloud computing* « nationales » en conformité avec la réglementation locale ? En France par exemple, SFR a signé un partenariat avec HP pour développer des offres de *cloud* à destination des PME. Avec EMC et VMWare, ATOS a créé Canopy, une société dédiée au *cloud computing*. La même société de services informatiques a également signé un accord avec Microsoft pour le déploiement des offres *cloud* de l'éditeur. Au terme de ces accords, la souveraineté des données peut également être garantie, ainsi que leur localisation : en l'occurrence, elles seront hébergées dans les « data centers » des acteurs nationaux situés sur le territoire de l'Etat membre concerné.

6 Le cadre juridique du *cloud computing*

Au moment où cette partie du rapport est écrite (mars 2013), il n'y a pas de dispositions réglementaires particulières relatives au c*loud* computing. Le phénomène, tout comme celui de la généralisation des réseaux sociaux, des moteurs de recherche et du *cloud* « grand public » (courrier électronique comme Gmail, Hotmail, boîtes de transfert comme Drop box) est apparu récemment et s'il y a une jurisprudence récente en la matière, celle-ci se fonde davantage sur la violation des règles du droit d'auteur (reprise des articles de presse dans les moteurs de recherche et les news ; tentative de fermetures de sites de partage de fichiers couverts par le droit d'auteur) que sur la responsabilité spécifique des acteurs du *cloud*.

Cependant, un nouveau cadre juridique européen est en pleine élaboration et, s'il est adopté durant la période 2013-2015, il produira pleinement ses effets durant les années qui suivront.

6.1 Situation en Belgique

A l'heure actuelle, il n'y a pas en droit belge de réglementation tout à fait propre au c*loud* computing. Il faut donc se référer aux règles générales qui régissent les obligations contractuelles, aux règles spécifiques qui régissent la protection des données et au régime de la responsabilité des hébergeurs de données.

6.1.1 La protection des données à caractère personnel

C'est le domaine de la protection des données à caractère personnel qui présente le plus de spécificités. Ce domaine fera prochainement l'objet d'une réforme européenne.

La protection des personnes à l'égard du traitement automatisé des données à caractère personnel a fait l'objet d'une convention du Conseil de l'Europe dès 1981[18].

Ensuite, c'est la loi belge du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel qui a défini les droits et devoirs de la personne responsable du traitement ainsi que ceux des personnes concernées par ces données :

- Devoir de transparence à la charge du responsable du traitement de données à caractère personnel ;
- Règles d'utilisation des données personnelles ;
- Nouveaux droits (accès, rectification, opposition) pour les personnes concernées.

[18] La Convention 108 du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.

Ultérieurement, c'est le droit européen qui a pris le relai avec une série de directives qui se sont vues transposées dans les législations nationales :

- La directive 95/46/CE donne le régime général de la protection des données à caractère personnel et constitue la principale norme européenne en la matière, sur tout le territoire de l'Union ;
- La directive 97/66/CE qui concerne en particulier le domaine des télécommunications. Cette directive a depuis été abrogée/remplacée par la directive 2002/58/CE dite « vie privée et communications électroniques » qui met en œuvre les principes de la directive 95/46/CE dans le domaine des communications électroniques ;
- La directive 2006/24/CE qui établit les conditions dans lesquelles les données devront être traitées dans les Etats membres.

En droit belge, par le jeu des transpositions qui ont adapté la loi de 1992, les normes suivantes sont applicables :

Loi du **8 décembre 1992** - Protection de la vie privée à l'égard des traitements de données à caractère personnel
Transposition de la directive 95/46/CE : - Loi du 11 décembre 1998 - Arrêté royal du 13 février 2001 - Loi du 26 février 2003
Transposition de la directive 2002/58/CE : - Loi du 13 juin 2005 relative aux communications électroniques
Cas spécifique : - Protection de la vie privée des travailleurs (AR 12 juin 2002 rendant obligatoire la convention collective n° 81 du 26 avril 2002)

Tableau 2 – Normes belges (protection des données)

La directive 95/46/CE n'était pas applicable directement au niveau national. Elle devait donc être transposée par chaque Etat, ce qui a laissé le champ libre à de multiples variations. Par conséquent, la même situation ne sera pas réglementée identiquement en Belgique, en France, en Grande-Bretagne ou en Allemagne. Cela crée des problèmes pour les entreprises transnationales.

De plus, en 1995, il n'était pas encore question du « *cloud computing* ». En particulier, on ne prévoyait pas la globalisation du marché et la mobilité des données qui en découle.

Il était donc temps d'adapter, d'harmoniser et de renforcer le cadre légal existant. C'est pourquoi la Commission a publié le 25 janvier 2012 une proposition de règlement qui, une fois adoptée, devrait remplacer la directive 95/46/CE avec l'avantage d'être directement applicable dans les 27 (ou bientôt 28) Etats membres (ainsi qu'en certains Etats de l'AELE : Norvège, Islande et Liechtenstein qui font partie de l'EEE). Il n'y aura donc plus alors de différence de législation entre les Etats participants à ce régime.

Ces nouveaux éléments sont détaillés dans la section 6.2.

Quels sont, sur base du droit actuel, les principes applicables au c*loud* computing (pour les données à caractère personnel) ?

Le client du *cloud* computing, qui confie des données à un fournisseur externe (sous-traitant) est, et reste le contrôleur de ses données, c'est-à-dire en droit belge le « Responsable du traitement » (LVP 1 §4).

Le fournisseur de *cloud* est considéré comme un simple « sous-traitant », et c'est le client du *cloud* qui est responsable de la protection des données.

Toutefois, cela n'exonère pas le sous-traitant de toute responsabilité :

- Le sous-traitant est défini par la LVP comme la personne (physique ou morale), l'association de fait ou l'administration publique qui traite des données à caractère personnel pour le compte du responsable du traitement (LVP 1 §5) ;
- Dans le cadre de la protection des données, ce fournisseur de *cloud* n'est pas un tiers. Il est donc directement tenu par les dispositions de la loi (LVP 1 §6) ;
- Le responsable du traitement (client du cloud) sera tenu de choisir un sous-traitant qui apporte des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements (LVP 16 §1)[19] . La relation contractuelle entre le client et le fournisseur du cloud doit faire l'objet d'un contrat écrit, lequel doit mentionner la responsabilité du sous-traitant et convenir que le fournisseur du cloud est tenu par les mêmes obligations (que son client responsable du traitement) en ce qui concerne l'accès aux données et à leur protection (LPV 16 §1, 2° à 5°).
  Dans le cas du cloud computing où beaucoup de contrats sont des contrats d'adhésion mis en place par le seul fournisseur, la responsabilité d'établir un tel contrat est certes partagée entre les parties, mais on peut affirmer que le fournisseur de cloud, dont c'est l'activité principale, porte l'essentielle responsabilité de l'établissement de ce contrat ;
- Indépendamment de tout contrat, le fournisseur de *cloud* a de toute façon :
  - L'interdiction de faire quelque traitement que ce soit sans avoir reçu instruction du client (responsable du traitement), sauf en cas d'une obligation imposée par ou en vertu d'une loi, d'un décret ou d'une ordonnance (LVP 16 §3) ;
  - L'obligation comme sous-traitant de prendre les mesures techniques et organisationnelles requises pour protéger les données à caractère personnel contre la destruction accidentelle ou non autorisée, contre la perte accidentelle ainsi que contre la modification, l'accès et tout autre traitement non autorisé de ces données (LVP 16 §4).

[19] Modifié par la loi du 11.12.1998 – en vigueur le 01.09.2001.

Il ressort donc de ces dispositions que la responsabilité du fournisseur de *cloud* est importante, au cas où :

- Il aurait négligé de demander à son client si des données à caractère personnel faisaient l'objet de la sous-traitance ;
- Il aurait négligé ou rendu plus difficile la négociation d'un contrat écrit mentionnant sa responsabilité et le détail des mesures techniques prises pour assurer la protection des données ;
- Il aurait effectué des traitements sans l'autorisation du client (par exemple le transfert des données vers un pays tiers est une forme de traitement : c'est techniquement une « communication par transmission » un « enregistrement » et une « conservation », toutes ces opérations étant considérées comme un traitement selon la LVP 1 §2) ;
- Il aurait négligé (que ces mesures soient ou non détaillées dans le contrat) de prendre les mesures techniques et organisationnelles appropriées pour protéger les données contre la destruction, la perte, la modification, l'accès ou tout autre traitement non autorisé.

6.1.2 Le régime des transferts

Les données – qu'elles soient à caractère personnel ou non - doivent pouvoir circuler librement à travers l'Union européenne (et l'Espace économique européen associé). Ce qui peut poser problème, et que nous appellerons « transfert » (ou flux transfrontière) est une transmission de données personnelles qui est effectuée depuis un Etat membre vers un pays tiers, c'est-à-dire un pays qui n'est membre ni de l'Union européenne, ni de l'Espace économique européen[20].

Le transfert vers un pays tiers est autorisé, si le pays a un niveau de protection adéquat. Par contre, il ne peut être effectué vers un pays tiers ne disposant pas d'un tel niveau de protection, sauf dérogations limitativement énumérées.

Quels sont les pays tiers offrant un niveau de protection adéquat ?

La Commission en publie la liste sur son site[21]. Elle se base sur la législation générale et sectorielle du pays en question et de ses règles professionnelles. Il s'agit de la Suisse, du Canada (pour les traitements soumis à la loi canadienne « Personal Information Protection and Electronic Documentation Act »), de l'Argentine, des Etats-Unis (à condition que le destinataire des données aux Etats-Unis ait adhéré aux « principes de la sphère de sécurité » ou « Safe Harbor Principles »), de Guernesey, de l'île de Man, des îles Féroé, Jersey et Israël.

Le fournisseur de *cloud* dont l'infrastructure s'étend à travers ces pays peut donc – principalement si ses sites sont répartis entre l'Europe et les Etats-Unis ou le Canada – y faire circuler les données de ses clients.

[20] Commission de la protection de la vie privée – questions fréquentes - http://www.privacycommission.be/fr/faq-page/374#t374n7382.
[21] http://ec.europa.eu/justice/data-protection/index_fr.htm.

En ce qui concerne plus particulièrement les Etats-Unis, il faut que le fournisseur de *cloud* (s'il transfère vers un établissement filial du même groupe ou un sous-contractant) s'assure d'une adhésion effective de son groupe ou de son sous-contractant aux principes de l'accord « Safe Harbor ».

> « Safe Harbor » (en français « sphère de sécurité ») est le nom d'un accord de novembre 2000 entre l'UE et les Etats-Unis pour régler le transfert de données à caractère personnel de citoyens européens, de manière compatible avec les directives européennes. Cela permet à une entreprise américaine de certifier qu'elle respecte la législation de l'Espace économique européen (EEE) afin d'obtenir l'autorisation de transférer des données personnelles de l'EEE vers les Etats-Unis. L'accord impose les obligations suivantes :
>
> - Notification - Les individus situés dans l'EEE doivent être informés du fait que leurs données sont collectées et de la façon dont ces données vont être utilisées.
> - Choix - Les individus doivent avoir la possibilité de refuser que les données les concernant soient transférées à des tiers ou utilisées dans un but autre que celui auquel la personne a consenti précédemment.
> - Transfert à des tiers - Le transfert de données à des tierces parties ne peut se faire que vers un tiers garantissant le même niveau de respect des principes de protection de données personnelles.
> - Sécurité - L'entreprise prendra les mesures nécessaires pour protéger les informations collectées contre la suppression, le mauvais usage, la divulgation ou l'altération de ces données.
> - Intégrité des données - L'entreprise s'engage à n'utiliser les données collectées que dans le but pour lequel l'utilisateur a donné son accord.
> - Accès - Les individus doivent pouvoir accéder aux informations les concernant, et pouvoir les corriger ou les supprimer s'ils le souhaitent.
> - Application - L'entreprise mettra tout en œuvre pour que ces règles soient effectivement appliquées et contrôlera leur respect.
>
> Une entreprise américaine peut faire appel à un tiers pour contrôler sa « certification », mais elle peut aussi annoncer son adhésion à l'accord et contrôler elle-même qu'elle et son personnel sont formés et se conforment aux obligations. Ceci doit être fait chaque année.

Les transferts autorisés dans la sphère de sécurité « Safe Harbor » peuvent être effectués comme s'il s'agissait d'un transfert entre deux centres « *cloud* » tous deux situés en Belgique, ou dans un autre pays de l'Union européenne. Il faudra néanmoins toujours respecter les principes généraux de la loi (notamment de légitimité, compatibilité de la communication des données à un tiers avec le traitement d'origine, information des personnes concernées).

Que faire si le pays de destination n'est pas dans la liste publiée par la Commission ?

Si le pays où l'on souhaite transmettre des données n'est pas repris dans la liste des pays offrant un niveau de protection adéquat, le fournisseur de c*loud* (= le responsable du traitement, qui est dans le cas présent un transfert) peut offrir par la voie contractuelle, une protection appropriée. Cette protection peut ainsi être définie au moyen d'un contrat liant celui qui envoie les données et celui qui les reçoit et contenant des garanties suffisantes au regard de la protection des données. Toutefois, afin d'être appliqué en Belgique, ce contrat ou type de contrat doit être autorisé par un arrêté royal après avis de la Commission de la protection de la vie privée.

Il existe des modèles de contrats-type proposés par la Commission européenne[22] qui sont automatiquement considérés comme offrant des garanties suffisantes au regard de la protection des données (et ne doivent donc pas être autorisés par arrêté royal, s'ils sont utilisés comme tels sans modification). Une copie de ces contrats devra néanmoins être communiquée à la Commission de la protection de la vie privée afin qu'elle puisse s'assurer de sa concordance avec les modèles.

Les sociétés multinationales qui désirent réaliser des flux intra-groupe et dont certains membres sont établis en dehors de l'Espace économique européen dans un pays qui n'a pas été reconnu comme « offrant un niveau de protection adéquat » peuvent également offrir des garanties suffisantes de protection des données grâce à des règles d'entreprise contraignantes (Binding Corporate Rules - BCR[23]). Ces règles doivent être validées par les différentes autorités nationales de protection des données concernées par le flux (en Belgique, un arrêté royal doit être adopté, après avis de la Commission de la protection de la vie privée). Il existe également sur le site de la Commission européenne une section dédiée aux BCR et sur les divers outils élaborés par le groupe de travail « Article 29 » pour faciliter la tâche des entreprises[24].

Pour que les BCR soient considérées comme offrant des garanties suffisantes quant au respect de la protection des données, il faut qu'elles soient autorisées par les autorités nationales de protection des données compétentes. Une procédure de coopération entre les différentes autorités nationales a été élaborée par le groupe de travail « Article 29 » et elle permet à la société multinationale d'introduire sa demande auprès d'une autorité nationale unique qui prendra contact avec les autres autorités concernées dans l'Union européenne, pour permettre un examen concerté du projet de règles, et pour favoriser des décisions cohérentes des différentes autorités de protection des données sur le projet de règles d'entreprises contraignantes[25].

Les exceptions

En l'absence de contrat, il existe certaines « exceptions » qui permettent le flux de données vers des pays tiers. C'est notamment le cas lorsque les personnes concernées donnent leur consentement indubitable au transfert de leurs données vers un pays déterminé, ou lorsque le transfert est nécessaire pour exécuter un contrat avec la personne concernée, ou lorsque les données proviennent d'un registre public destiné à l'information du public (annuaire téléphonique, registre du commerce, par exemple). Ces exceptions doivent être interprétées de manière restrictive et ne peuvent constituer un cadre normal de flux de données, notamment lorsque ceux-ci sont massifs ou répétitifs.

[22] Le modèle a été adopté par décision de la Commission du 5 février 2010 (document C (2010) 593). Il n'existe qu'en langue anglaise : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:006:0052:0062:en:PDF.

[23] Une BCR est une règle élaborée par une entreprise multinationale (tel un code de conduite interne) qui doit être obligatoire pour l'ensemble de ses entités et employés et qui porte sur les transferts internationaux de données personnelles qui sont réalisés au sein du groupe. http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/index_en.htm.

[24] http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/tools/index_en.htm.

[25] Document de travail du 14.4.2005 relatif à une procédure de coopération en vue de l'émission d'avis communs sur le caractère adéquat de la protection offerte par les « règles d'entreprise contraignantes » (WP107).

Elles ne peuvent donc constituer qu'un palliatif d'urgence et il faut rapidement mettre en place une solution contractuelle qui formalise les garanties de protection des données.

6.1.3 Quelle est la « loi applicable » au traitement des données ?

La détermination de la loi applicable est importante pour que les clients du cloud (responsables du traitement ou « contrôleurs ») puissent apprécier leurs obligations dans un cadre déterminé. On notera que cette loi est à distinguer de la juridiction compétente (le for) en cas de plainte ou litige, qui ne sera pas nécessairement identique : un juge étranger peut donc être amené à se prononcer sur un cas d'application de la loi belge. La loi applicable peut différer selon qu'il s'agisse du traitement des données ou d'autres impératifs comme la sécurité.

En matière de protection des données personnelles, la loi applicable (comme résultant de la directive 95/46), est liée au responsable du traitement, et non à l'endroit où les données sont traitées ou stockées, ce qui convient bien dans le cadre du *cloud* computing car cet endroit n'est pas toujours déterminable[26]. Il n'y a donc pas de différence si un client établi en Belgique stocke ses données en Belgique, dans l'UE ou même hors UE : la loi belge devra s'appliquer dans tous ces cas.
Il suffit donc que le « contrôleur » (responsable du traitement) ait un « établissement » sur le territoire de l'UE ou y utilise des « équipements » ou « moyens » (article 4.1 c de la directive). La situation peut se compliquer dans les cas où le fournisseur de cloud est aussi responsable du traitement (il fournit par exemple un agenda en ligne où les particuliers peuvent enregistrer leurs rendez-vous, un réseau social ou un espace de stockage où on peut stocker ses données, etc.) et où il n'a pas d'établissement dans l'UE. Il faut alors être attentif au fait que ce fournisseur utilise dans l'UE des équipements ou moyens. Comme le relève le groupe de travail « Article 29 », cela nécessite alors d'interpréter la notion de « moyen » un simple transit des données collectées (transfert par le réseau) ou l'utilisation de personnel (employé qui collecte les données) ou certaines formes de publicité (sollicitation en ligne depuis un site internet étranger) ne serait pas suffisant, tandis qu'un site établi dans l'UE, des voitures enregistreuses d'images, ou un équipement spécifiquement destiné à la collecte ou au traitement le seraient.

La situation est différente en matière de mesures de confidentialité et sécurité (article 17(3) de la directive, transposé dans l'article 16 LVP) : la loi applicable est celle du l'Etat membre où le processeur (fournisseur de cloud ou « sous-traitant ») est établi. Or, même à l'intérieur de l'UE, les exigences de sécurité varient fortement selon les Etats membres. Certains n'ont fait que reproduire les termes généraux de la directive (le responsable du traitement doit mettre en œuvre les mesures techniques et d'organisation appropriées… choisir un sous-traitant qui apporte des garanties suffisantes au regard des mesures de sécurité et d'organisation… veiller au respect de ces mesures), tandis que d'autres, comme la Belgique exigent des mentions contractuelles écrites, fixant la responsabilité

[26] Article 29 data protection Working Party, Opinion 8/2010 on applicable law
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_en.pdf

du fournisseur de *cloud*, lui imposant les mêmes obligations que le responsable du traitement.

La loi belge impose donc de meilleures garanties, qui doivent se retrouver dans un contrat écrit (ce contrat devenant la « loi des parties ») notamment au cas où une autre loi moins exigeante est applicable (loi d'un autre Etat membre si le fournisseur de *cloud* opère dans l'UE ou loi d'un Etat tiers s'il est établi hors UE). Ces dispositions se rapportent toujours à la sécurité des données à caractère personnel, alors que des clients peuvent mettre sur le *cloud* d'autres données à caractère confidentiel (par exemple une documentation relative aux objectifs stratégiques d'une entreprise ou à ses secrets de fabrication). C'est pourquoi il faut recommander aux clients de s'assurer dans tous les cas (et pas seulement pour la sous-traitance de données à caractère personnel) de la meilleure protection contractuelle. C'est une des raisons de la recommandation de clauses types (voir section 9).

6.1.4 La responsabilité du fournisseur de *cloud* qui héberge des données

L'hébergement par un fournisseur d'infrastructure *cloud* peut couvrir toutes sortes de données (documents, fichiers, enregistrements musicaux, photos, vidéos) que l'on ne peut pas nécessairement qualifier de données à caractère personnel, mais qui peuvent aussi, ou en outre :

- être « illicites ***par violation*** du droit des tiers », c'est-à-dire faire l'objet de droits divers, principalement intellectuels (en particulier les droits d'auteur) qui peuvent être violés du fait de la copie, détention, communication ou distribution de ces données ;
- être « illicites ***par nature*** » c'est-à-dire interdites de détention, traitement ou diffusion par la loi (on pense ici particulièrement aux images ou films à caractère sexuel mettant en scène des mineurs, des crimes ou des actes pédophiles/la pédopornographie) ;
- être « illicites ***par destination*** » c'est-à-dire servir à organiser ou à documenter une activité illicite : le terrorisme, l'espionnage, le trafic de drogues, le proxénétisme, la traite des êtres humains, le recel ou la vente d'œuvres volées, le trafic d'armes, etc.

Cette responsabilité a été mise en place par les lois du 11 mars 2003 sur certains aspects juridiques des services de la société de l'information[27]. Aux termes de cette loi, l'activité d'hébergement est définie comme la « fourniture d'un service de la société d'information – c'est-à-dire tout service presté normalement contre rémunération, à distance, par voie électronique et à la demande individuelle d'un destinataire du service - consistant à stocker des informations fournies par un destinataire du service ».

Ici encore, bien que ni la directive, ni la loi ne visent expressément le *cloud* computing, on peut faire l'assimilation suivante :

[27] Cette loi belge transpose la directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (communément appelée « directive sur le commerce électronique »).

Fournisseur d'un service de la société de l'information	= *Cloud* provider = Fournisseur de *cloud*
Destinataire du service	= *Cloud* customer = Client du *cloud*

L'article 20 de la loi qui transpose les termes de la directive stipule que l'hébergeur (le fournisseur de *cloud*) peut ne pas être responsable des informations stockées à la demande d'un destinataire du service (son client du *cloud*), mais seulement sous certaines conditions :

- Il ne peut pas avoir une connaissance effective de l'activité ou de l'information illicite, ou de circonstances pouvant faire apparaître le caractère illicite de l'activité ou de l'information. Cette méconnaissance pourrait être difficile à affirmer, par exemple si le fournisseur de *cloud* a organisé un service d'application (SaaS) spécifiquement destiné au partage, à l'échange et à la distribution de films ou d'enregistrements musicaux. De même, si d'une manière ou d'une autre l'hébergeur a participé activement à la diffusion de l'information, il ne pourra s'exonérer[28] ;
  Il doit agir promptement dès le moment où il a une telle connaissance, pour retirer les informations ou rendre l'accès à celles-ci impossible ;
  Il doit informer immédiatement le procureur du roi. Cela ne transforme pas le fournisseur du *cloud* en « policier », car il n'a pas d'obligation générale de « surveillance active » ni de « prévention des infractions »[29] mais il doit bien agir « sur-le-champ », c'est-à-dire dès qu'il a eu connaissance des faits[30].

Sans que l'on puisse donc lui demander une surveillance systématique, il résulte des dispositions qui précèdent que le fournisseur de *cloud* devrait avoir une idée générale des données qu'on lui confie et, à tout le moins dans son contrat de service, obtenir formellement du client l'assurance que l'information transmise, conservée et/ou diffusée ne présente aucun caractère illicite (que ce soit par nature, par destination ou du fait de la violation du droit des tiers).

[28] La Cour d'appel de Bruxelles a refusé à Google la qualité d'hébergeur exonéré de responsabilité dans le cadre de son onglet « Google Actualités » car elle a estimé que Google éditait activement ces pages - Bruxelles, 5 mai 2011, disponible sur www.juridat.be; 2007/AR/1730.
[29] Saisie par les tribunaux belges, la Cour de Justice de l'Union européenne a confirmé qu'on ne pouvait pas imposer d'obligation générale de surveillance aux hébergeurs (par exemple en leur imposant un contrôle préventif ou systématique de toutes les données stockées par les clients) : affaire Sabam c/ Tiscali-Scarlet, Civ. Bruxelles (cess), 29 juin 2007, disponible sur http//www.droit-technologie.be + CJUE 24 novembre 2011 C-70/10 et affaire Sabam / Netlog, CJUE, 16 février 2012, C-360/10.
[30] Le §3 de l'article 20 de la loi prévoit que « *lorsque le prestataire a une connaissance effective d'une activité ou d'une information illicite, il les communique sur le champ au procureur du Roi qui prend les mesures utiles conformément à l'article 39 bis du Code d'instruction criminel* » (relatif à la saisie de données immatérielles).

6.1.5 Le cas particulier des communications électroniques

On assiste à une évolution rapide des « applications *cloud* » et les réseaux sociaux d'aujourd'hui semblent, selon certaines études, prendre une part de plus en plus importante dans les communications électroniques[31].

Dans ce cadre, le fournisseur de *cloud* sera tenu par les dispositions qui découlent de la transposition de la directive « vie privée et communications électroniques »[32]. Cette directive a été adoptée en 2002 en même temps qu'un nouveau dispositif législatif appelé à encadrer le secteur des communications électroniques. Elle contient des dispositions sur un certain nombre de thèmes plus ou moins sensibles, tels que la conservation des données de connexion par les Etats membres à des fins de surveillance policière (rétention des données), l'envoi de messages électroniques non sollicités (spam), l'usage des témoins de connexion (« cookies ») et l'inclusion des données personnelles dans les annuaires publics.

6.2 Le cadre européen (situation actuelle et projets)

Le *cloud* computing est un phénomène qui sera abordé par de nombreux domaines de la politique européenne. Cela va de la protection du consommateur, aux règles relatives aux contrats, au commerce électronique, à la standardisation et à la certification d'entreprises, jusqu'à divers aspects de la protection de la vie privée.

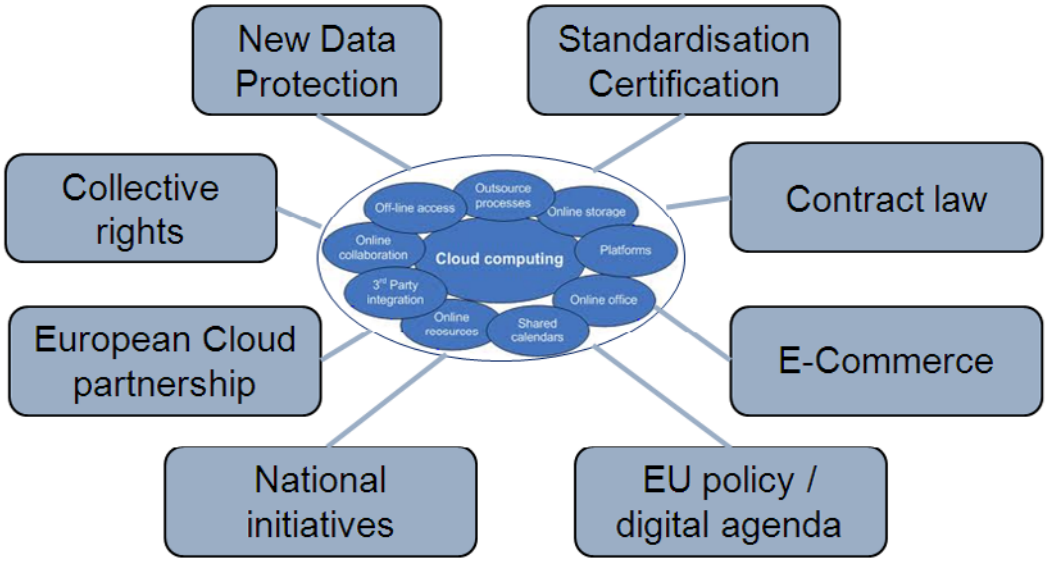

Figure 10 – Le cloud et les évolutions en cours

[31] Voir « Les réseaux sociaux ont détrôné l'e-mail aux Etats-Unis » http://www.lemonde.fr/technologies/article/2011/02/08/les-reseaux-sociaux-ont-detrone-les-mails-aux-etats-unis_1476656_651865.html.

[32] Directive 2002/58/CE du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive « vie privée et communications électroniques ») - Journal officiel L 201 du 31 juillet 2002.

Le domaine de la protection de la vie privée semble le plus visible et le plus problématique, ainsi qu'en témoigne un grand nombre d'études et de positions politiques publiées. C'est la raison pour laquelle nous en parlons en premier lieu.

6.2.1 Le cadre de la protection des données

Droit applicable

Dans l'Union européenne, les questions relatives au traitement des données personnelles par des moyens informatiques sont réglées par la directive UE 95/46 sur la protection des données[33]. La directive UE 2002/58 sur la protection des communications électroniques[34] mise à jour par la directive UE 2009/136[35] s'applique au traitement de données personnelles quand on offre des services de communication au public et est dès lors applicable au cas où ces services sont fournis au moyen d'une solution de type *cloud*.

L'article 4 de la directive 95/46/UE note que les réglementations nationales qui transposeront la directive seront applicables au traitement de données si le responsable du traitement des données est établi sur le territoire d'un ou plusieurs Etats membres de l'Union ou si les équipements utilisés se trouvent sur le territoire de l'Union.

Le responsable du traitement et le « processeur » des données : rôles, droits et responsabilités

Afin d'aborder les questions relatives aux responsabilités et aux obligations des différents acteurs dans le domaine du *cloud* computing, il faut tout d'abord définir les concepts du « responsable du traitement » (en anglais « data controller ») et du « sous-traitant » (appelé en anglais « data processor », celui qui fournit les ressources informatiques nécessaires). Etant donné que le client du *cloud* prend les décisions importantes relatives au traitement (son objectif ou la délégation d'activités de traitement au sous-traitant), il est supposé agir en tant que responsable du traitement. Le fournisseur de *cloud* (« *cloud* provider ») est l'organisation qui fournit les services de *cloud* computing (les moyens et la plateforme), agissant au nom du client du *cloud*, et donc agissant en tant que sous-traitant.

Dans son Opinion sur le *Cloud* Computing[36], validée le 1er juillet 2012, le groupe de travail « Article 29 » sur la protection des données (Art. 29 WP) argumente que beaucoup

[33] Directive 95/46/EC du Parlement européen et du Conseil du 24 Octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, JO L 281 de 23.11.1995 p. 31.
[34] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.07.2002, p. 37.
[35] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, OJ L 337 of 18.12. 2009 p. 0011 – 0036.
[36] Article 29 Data Protection Working Party, WP196 – Opinion 05/2012 on Cloud Computing, adopted July 1st 2012, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinionrecommendation/index_en.htm#h2-1.

de clients actuels de services de *cloud* computing semblent considérer qu'ils n'ont que peu de possibilité pour négocier les conditions contractuelles à cause des offres standardisées. Cependant, le client a en tout cas le droit de choisir un fournisseur de *cloud* et il devrait choisir celui qui agit strictement selon les exigences dans le domaine de la protection des données. Comme confirmé par le groupe de travail « Article 29 », validé au préalable dans l'Opinion 1/2010 sur les concepts de « responsable du traitement » et de « sous-traitant »[37], « l'existence d'une loi protectrice ne devrait pas être considérée comme excuse ou une protection suffisante permettant au responsable du traitement d'accepter n'importe quelles conditions contractuelles qui reflèteraient un déséquilibre entre le pouvoir d'un petit responsable de traitement face à un gros fournisseur de services ».

Une des obligations importantes que les fournisseurs de *cloud* doivent garantir est la confidentialité du traitement. Les sous-traitants doivent prendre en considération le type de *cloud* (p. ex. public, privé, communautaire ou hybride) ainsi que le type de service stipulé par contrat. Ils sont obligés d'implémenter des mesures de sécurité conformes aux normes de l'UE. Qui plus est, les sous-traitants doivent assister le responsable du traitement dans l'observation des droits relatifs aux sujets des données.

Il faut noter que toutes les obligations pertinentes dans le domaine des services de *cloud* computing s'appliquent également aux sous-contractants du fournisseur de *cloud* (les « sub-processors » des données) ; les contrats entre le fournisseur de *cloud* et des sous-contractants devraient être basés sur les conditions du contrat initial entre le client du *cloud* et le fournisseur du *cloud*.

Evolution attendue : un nouveau règlement général

Afin d'établir quelques garanties au niveau des sous-contractants, la Commission a introduit des dispositions nouvelles dans sa proposition de 2012 pour un règlement général sur la protection des données[38].

Pourquoi un règlement ? Pour éviter qu'une nouvelle directive ne soit transposée avec des variantes ou ajouts différents selon les Etats membres. Le règlement sera le premier instrument international contraignant ayant pour usage la protection des données à caractère personnel contre l'usage abusif du traitement automatisé des données à caractère personnel.

De manière générale, la proposition de règlement renforce les droits des personnes concernées par le traitement de leurs données personnelles et impose de nouvelles obligations aux entreprises responsables de traitement.

Le projet démontre que la Commission européenne n'entend pas se limiter à un simple toilettage du cadre légal existant, mais entreprend d'harmoniser le cadre légal, de

[37] Opinion 1/2010 on the concepts of "controller" and "processor" http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf.
[38] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 25.1.2012.

renforcer les droits des personnes concernées et de rendre le respect de la réglementation plus effectif sur les points suivants :

1. Harmoniser et actualiser

Le cadre légal actuel qui a vu le jour en 1995 n'était pas applicable directement au niveau national. Chaque Etat membre l'a donc transposé dans sa propre législation en profitant des libertés concédées. Il en résulte des divergences notables dans le droit des pays de l'Union. Une situation identique ne sera donc pas réglée légalement de la même manière entre, par exemple, l'Italie, l'Allemagne, le Royaume-Uni et la Belgique. Une entreprise présente dans ces quatre pays devra soumettre ses opérations à des textes légaux différents sur certains points, alors que bien souvent cette entreprise collecte et échange un nombre important de données personnelles via et entre ses différents sièges.

Le second inconvénient tient au fait que la directive est née avant notamment l'avènement des réseaux sociaux et du *cloud* computing. Ces éléments, s'ils ne sont pas à eux seuls déterminants dans l'évolution du traitement de données personnelles, traduisent en tout cas l'explosion et la globalisation du traitement de données personnelles durant cette dernière décennie.

2. Renforcer la protection des personnes concernées

La protection des sujets des données (appelés « personnes concernées ») est renforcée dans le projet de règlement par :

- Une application extraterritoriale : alors que la directive actuelle prévoit des critères de rattachement presque physiques entre la personne concernée et un Etat participant pour que la réglementation européenne s'applique, le projet de règlement prévoit une application extraterritoriale du droit européen. C'est ainsi que les exigences d'un « *établissement* » du responsable ou de son sous-traitant sur le territoire de l'Union, ou de la présence de « *moyens automatisés ou non* » sur le territoire de l'Union disparaissent. La nouvelle réglementation s'appliquera donc pour tout opérateur qui dirigerait ses activités de traitement vers l'Union, même en l'absence d'établissement dans l'Union ou de moyens localisés sur ce territoire ;

- Une clarification du droit à l'oubli, c'est-à-dire de voir des données effectivement supprimées quand leur conservation n'est plus souhaitable. Ce droit est particulièrement utile dans le cadre de l'utilisation des réseaux sociaux ;

- Un droit nouveau à la « *portabilité* » des données, qui va donner la possibilité au client du *cloud* d'exiger que ses données soient détenues dans un format (par exemple un standard ouvert) lui permettant de les transférer vers un autre fournisseur de *cloud* ;

- Une clarification de certaines notions comme la « personne concernée » (dont les données sont traitées) qui est toute personne pouvant être identifiée, directement ou indirectement, par le responsable du traitement lui-même ou par toute autre personne physique ou morale (ce peut donc aussi être une personne dont l'image a été prise, éventuellement à son insu, pour être ensuite traitée dans le *cloud*,

publiée sur un réseau social etc.), et le « consentement » qui est l'indication d'une volonté spécifique, éclairée et explicite, donnée librement (ce qui peut viser tant les mineurs, pour lesquels il faudra l'accord d'un parent, ou d'autres personnes dont la liberté est limitée – par exemple par un contrat de travail).

3. Renforcer les obligations et les sanctions

Les obligations nouvelles créées par le projet de règlement portent sur la nomination d'un « agent qualifié responsable des données personnelles » dans les entreprises de plus de 250 travailleurs, sur l'obligation de dresser dans certains cas un rapport relatif à l'impact du traitement envisagé sur la protection des données, sur la documentation des politiques et protections mises en place, ainsi que des opérations effectuées, sur les notifications des problèmes (par exemple de perte de données) à l'autorité nationale de protection des données personnelles et dans certains cas à la personne concernée. Enfin, il y a un renforcement des sanctions qui peuvent s'élever jusqu'à 5 % du chiffre d'affaires annuel mondial du responsable de traitement en cas de contravention.

Dispositions concernant plus particulièrement le fournisseur de *cloud*

Dans l'article 26(2) de la proposition de règlement, l'intervention d'un sous-traitant sera régie par un contrat ou tout autre document légalement contraignant, liant le sous-traitant au responsable du traitement, et précisant en particulier que le sous-traitant (par exemple le fournisseur de *cloud*) ne peut lui-même sous-traiter à un tiers qu'avec la permission préalable du responsable de traitement.

Comme expliqué ci-dessus, la validité du traitement de données personnelles dans le *cloud* dépend de la conformité des règles EU relatives à la protection des données. Celles-ci incluent la transparence du traitement des données envers le sujet des données, le principe de la limitation du traitement à son but, l'obligation de corriger les données si nécessaire et de les supprimer quand la conservation n'est plus nécessaire. Qui plus est, il faut implémenter des mesures techniques et d'organisation adéquates afin de garantir la protection et la sécurité des données. Outre les exigences de sécurité principales au niveau de la disponibilité, de la confidentialité et de l'intégrité, il faudrait prendre en considération des critères supplémentaires comme la transparence, l'isolation, la possibilité d'intervenir, la responsabilité quant aux dommages éventuels causés et la portabilité. Selon l'article 17(3) de la directive 95/46/EC, un contrat formellement signé avec le fournisseur de service *cloud* devrait inclure des dispositions relatives à ces mesures de sécurité.

En général, le contrat devrait couvrir les questions suivantes, comme stipulé par le groupe de travail « Article 29 » :

1) Détailler les demandes ou attentes du client du *cloud* envers son fournisseur, en particulier concernant le contrat de niveau de services applicable (SLA, qui doit être objectif et mesurable) et les pénalités applicables (sommes à payer pour compenser un dommage et possibilité d'action envers le fournisseur en cas de non-conformité).
2) Spécifier les mesures de sécurité auxquelles le fournisseur de *cloud* doit se conformer.

3) Préciser la nature des services et la période couverte par les services du fournisseur de *cloud*, l'étendue, la manière et le but des traitements de données à caractère personnel ainsi que le type de données personnelles traitées.
4) Préciser les conditions de restitution des données personnelles et leur destruction (sur le site du fournisseur de *cloud*) un fois que le service sera terminé.
5) Inclure une clause de confidentialité contraignante pour le fournisseur de *cloud* et tous ses préposés qui auraient accès aux données.
6) Inclure l'obligation pour le fournisseur de *cloud* de porter assistance à son client pour faciliter l'exercice par les personnes concernées de leur droit d'accès, de rectification ou de suppression de leurs données.
7) Etablir de manière formelle que le fournisseur de *cloud* ne peut communiquer les données à des tiers, même pour des motifs de sauvegarde, sauf si le contrat prévoit la possibilité pour le fournisseur de sous-contracter ces services.
8) Préciser les responsabilités du fournisseur concernant la notification au client du *cloud* en cas d'atteinte aux données ou d'incident qui pourrait avoir un impact sur les données confiées par le client.
9) Obligation du fournisseur de *cloud* d'indiquer au client une liste des lieux physiques où les données pourront être traitées.
10) Droit pour le client du *cloud* (responsable du traitement) d'obtenir des informations lui permettant de vérifier le respect du contrat, et obligation pour le fournisseur de *cloud* d'y coopérer.
11) Obligation pour le fournisseur de *cloud* d'informer le client du *cloud* au sujet de changements significatifs concernant le service, tel que la mise en place de fonctionnalités additionnelles.
12) Description des opérations de traçage ou d'audit (logging and auditing) des traitements relatifs aux données à caractère personnel qui sont effectués par le fournisseur de *cloud* ou par ses sous-contractants.
13) Notification au client du *cloud* des demandes d'accès aux données auxquelles le fournisseur de *cloud* est légalement obligé de répondre, faites par les autorités judiciaires ou policières compétentes, sauf si cette notification est interdite par la loi, par exemple dans le but de préserver la confidentialité d'une enquête criminelle.
14) Obligation générale du fournisseur de *cloud* de donner l'assurance que son organisation interne et ses procédures de traitement des données sont conformes aux standards nationaux et internationaux applicables.

L'avertissement en cas de violation des données

Dans le projet de règlement général sur la protection des données, on propose d'imposer une clause demandant d'avertir les autorités de la protection des données ainsi que les sujets des données en cas de violation des données. Les dispositions du projet prévoient que les autorités de la protection des données doivent être informées « si possible » dans un délai de 24 heures ; les sujets des données en question par contre doivent être avertis dans un délai « approprié ». Le projet de règlement étend l'exigence relative à l'avis de violation des données des fournisseurs de services de télécommunications et d'internet dans l'UE à tous les secteurs d'activité ou d'affaires, ce qui est un pas en avant important compte tenu de l'augmentation des risques globaux dans le domaine de la criminalité informatique et des pertes de données.

Les transferts de données en dehors de l'EEE

Les articles 25 et 26 de la directive 95/46/EC comportent des dispositions de principe relatives au transfert de données personnelles vers des pays tiers et aux dérogations de ces principes. Le concept d'un niveau adéquat de protection de données permet de traiter des données en dehors de l'EEE si une telle protection est garantie. Autrement le responsable du traitement et/ou le fournisseur de *cloud* doivent répondre à des conditions spécifiques. Etant donné qu'il est rarement possible de situer les données dans un environnement *cloud*, l'application d'un cadre légal déterminé devient assez compliquée.

En premier lieu, les considérations relatives au niveau adéquat de protection ont des limites géographiques et ne peuvent par conséquent couvrir tous les transferts au sein du c*loud*. C'est également applicable aux critères définis par l'accord Safe Harbor. Le groupe de travail « Article 29 » considère en effet que la seule existence de la certification Safe Harbor (qui résulte le plus souvent d'une simple déclaration) ne suffit pas et que l'importateur des données devrait concrètement prouver que les principes relatifs à la protection de la vie privée ont été respectés. Qui plus est, il faut vérifier si les contrats établis par l'entreprise fournissant la solution *cloud* sont conformes aux dispositions légales nationales. En dernier lieu, il est peut-être nécessaire d'implémenter des mesures de précaution supplémentaires compte tenu du type spécifique du *cloud* (p. ex. certains risques de sécurité spécifiques au *cloud*, tels que de la suppression incomplète de données, pourraient ne pas être suffisamment pris en considération par les principes Safe Harbor existants relatifs à la sécurité des données).

Les clauses contractuelles standards (SCC) telles que validées par la Commission européenne afin de créer un cadre international pour les transferts de données[39] devraient également être mentionnées dans ce contexte. Quand le fournisseur de *cloud* agit en tant que sous-traitant (processeur des traitements[40]), les clauses modèles pourraient être utilisées dans son contrat avec le responsable du traitement afin d'offrir des mesures de protection adéquates dans l'environnement du *cloud* computing.

Un autre instrument à discuter consiste en les règles d'entreprise contraignantes (Binding Corporate Rules ou BCR) comprenant des lignes directrices pour les entreprises transférant des données au sein de leur groupe. De telles BCR permettent de transférer des données personnelles à l'entreprise du groupe qui effectue un traitement, tout en les gardant dans le domaine d'affaire du fournisseur de *cloud* et en bénéficiant du niveau de protection adéquat à travers tous les établissements du groupe.

Remarques et recommandations de conclusion

Dans son « Sopot Memorandum » de 2012 sur le *cloud* computing, l'International Working Group sur la protection des données dans la télécommunication estime entre autres que cette technologie est par nature « sans frontières et transfrontière » et que

[39] Decision 2010/87/EU of the European Commission of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, OJ L 39/5, 12.2.2010

[40] Le texte français de la directive traduit l'anglais « processor » par « sous-traitant ».

dans ce sens « le traitement des données est entré dans un monde global »[41]. C'est pour cette raison que les organisations qui souhaitent prendre leur place dans le marché des services de *cloud* computing devraient bien prendre en considération les risques pertinents sur le plan de la protection des données et devraient, en particulier, se concentrer sur les obligations relatives à la sécurité et aux transferts internationaux.

Le respect de la protection des données par les clients du *cloud* et par les fournisseurs du *cloud* devrait en premier lieu être basé sur le cadre légal actuel, c'est-à-dire la directive 95/46/EC. Ceci a également été confirmé lors de la réunion du 16 janvier 2013 entre les représentants de la Commission européenne de la DG Connect et l'équipe chargée de la présente étude[42].

Le but de cette réunion consistait à discuter de certains aspects de *cloud* computing tels que remarqués dans l'Agenda numérique pour l'Europe[43]. On a souligné qu'il faut surtout continuer à se concentrer sur les possibilités légales actuelles étant donné que de nouvelles règles relatives à la protection des données (telle la proposition du nouveau règlement) ne peuvent être traduites dans la réalité qu'après de nombreuses années.
Cependant, une remarque a été faite concernant les concepts du responsable du traitement et du « processeur » (sous-traitant) vu que le projet de règlement semble avoir laissé quelques imprécisions à ce sujet et on a donc proposé de travailler sur des lignes directrices explicatives. Cependant, se basant sur les recommandations de la DG Justice, on a décidé de plutôt inclure des explications possibles dans les actes d'implémentation ou de la délégation suite à l'adoption du règlement. Une telle solution semble être plus adéquate compte tenu du caractère changeant de l'environnement de *cloud* computing, vu que des stipulations trop détaillées peuvent à nouveau nécessiter des modifications à l'avenir.

Quant aux développements futurs dans le cadre régulateur du *cloud* computing, quelques recommandations ont été prévues par le groupe de travail « Article 29 » dans son Opinion, lesquelles méritent d'être mentionnées ci-dessous :

- Un meilleur équilibre des responsabilités entre le responsable du traitement et le fournisseur de *cloud* : l'article 26 du projet de règlement impose au fournisseur de prêter assistance au responsable en ce qui concerne le respect de la sécurité et de ses autres obligations. De plus, l'article 30 du projet introduit une obligation légale pour le fournisseur de *cloud* de mettre en place des mesures techniques et organisationnelles appropriées. Le projet prévoit aussi que si un sous-traitant (fournisseur de *cloud*) est en défaut de respecter les instructions du responsable du traitement, il devient responsable au même titre et est sujet aux mêmes règles de contrôle. Sur cette base, le groupe de travail « Article 29 » considère que le projet de règlement va dans la bonne direction pour remédier au déséquilibre qui caractérise souvent le *cloud* computing, où le client (spécialement s'il s'agit d'une

[41] International Working Group on Data Protection in Telecommunications, Working Paper on Cloud Computing – Privacy and Data Protection issues – "Sopot Memorandum, 675.44.8, Sopot, 24.3.2012.
[42] Meeting with the European Commission, DG CONNECT/E2 Software & Services, Cloud, Brussels, 16.01.2013.
[43] Communication from the Commission of 3 March 2010 - Europe 2020 A strategy for smart, sustainable and inclusive growth, COM(2010) 2020 final, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:2020:FIN:EN:PDF.

PME) peut éprouver des difficultés à exercer l'entier contrôle, requis par la loi sur la protection des données, concernant la manière dont le fournisseur de *cloud* délivre son service. Cependant, compte tenu de la situation juridique asymétrique des personnes concernées (sujets de données) et des petites entreprises face aux géants du *cloud* computing, il est recommandé de prévoir un rôle plus actif pour les organisations protégeant les consommateurs ou représentant les partenaires sociaux, qui doivent avoir le pouvoir de négocier des conditions générales plus équilibrées avec ces grands fournisseurs.

- En matière d'accès aux données par la sécurité de l'Etat ou les autorités de justice et police, le groupe de travail « Article 29 » estime que de nouvelles dispositions devraient être ajoutées au projet de règlement. Il estime que les responsables de traitement qui opèrent dans l'Union ne devraient jamais divulguer des données à caractère personnel aux autorités judiciaires ou administratives d'un Etat tiers, sauf si c'est autorisé dans le cadre d'un accord international, d'un traité d'assistance mutuelle ou approuvé par l'autorité de supervision (de l'Etat membre concerné). Dans son opinion, le groupe de travail « Article 29 » estime que le règlement du Conseil (EC) No 2271/96[44] pourrait servir de base légale. Le groupe de travail s'inquiète de ce manque dans le projet de règlement proposé par la Commission, car cela crée une incertitude juridique quand les données sont réparties dans des centres de traitement disséminés dans le monde. Pour cette raison, il suggère d'intégrer dans le règlement l'obligation de suivre la procédure prévue par les traités d'assistance judiciaire mutuelle (MLATs) dans les cas où la divulgation ne serait pas autorisée par la loi de l'Union ou de ses Etats membres.
  Cette recommandation est directement liée aux craintes exprimées envers la loi américaine « Patriot Act » qui donnerait au gouvernement américain un accès injustifié et sans contrôle aux données qui seraient conservées sur des serveurs de *cloud* gérés par des fournisseurs américains (ou ayant au moins un établissement aux Etats-Unis, ce qui les obligerait à répondre aux demandes d'accès des autorités américaines). Selon les considérations clés de l'étude du Parlement européen sur la lutte contre le crime informatique et la protection de la vie privée sur le *cloud*[45], ces questions de « privacy » et de protection des données ont été totalement négligées, tant dans le cas du « Patriot Act » que dans le cas du Foreign Intelligence Surveillance Amendment Act (FISAA) de 2008, malgré leur impact considérable sur la souveraineté de l'UE quant à ses données et sur la protection des droits des citoyens.
  Cependant, il faut noter que les experts de la Commission présents lors de la rencontre avec l'équipe de cette étude ont exprimé une opinion différente, se référant aux législations de certains Etats membres qui, selon eux, comportent dans cette matière des dispositions semblables, si ce n'est encore plus permissives ou intrusives. Par exemple, les autorités françaises compétentes en

[44]Council Regulation (EC) No 2271/96 of 22 November 1996 protecting against the effects of the extraterritorial application of legislation adopted by a third country, and actions based thereon or resulting therefrom, OJ L 309 , 29/11/1996 P. 0001 – 0006.
[45] Study on Fighting Cybercrime and Protecting Privacy in the Cloud, requested by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs; study conducted under coordination of the Justice and Home Affairs Section of the Centre for European
Policy Studies (CEPS) and the Centre d'Etudes sur les Conflits (C&C), 2012.

matière pénale peuvent obtenir l'accès aux données sans en informer la personne concernée. Des droits semblables à ceux établis par le « Patriot Act » sont reconnus aux autorités britanniques chargées de la répression. En outre, la nouvelle proposition d'une directive qui étend la protection due au traitement des données aux agences européennes chargées de missions judiciaires[46] a été citée comme illustrant une approche européenne cohérente et claire dans le domaine de la protection des données des individus, aussi bien en cas de répression ou prévention criminelle que dans les cas de coopération internationale.

- Précautions particulières à prendre par le secteur public : le groupe de travail « Article 29 » considère qu'il convient d'ajouter une mise en garde particulière concernant la nécessité qu'un organisme public évalue en premier lieu si la communication, le traitement et le stockage des données en dehors du territoire national peuvent présenter des risques inacceptables de sécurité et de protection de la vie privée pour les citoyens et pour la sécurité nationale et l'économie – en particulier lorsque des bases de données sensibles (comme les données de recensement) ou des services stratégiques (comme les soins médicaux) sont en jeu. Selon cette vision, ce point mérite d'être pris en considération chaque fois que des données confidentielles sont traitées dans le *cloud*. De ce point de vue, les gouvernements nationaux et les institutions de l'Union européenne pourraient envisager de poursuivre l'étude d'un « *cloud* gouvernemental européen » qui constituerait un espace virtuel supranational où pourraient s'appliquer des règles uniformes et harmonisées.

6.2.2 Le cadre de la protection du consommateur et de la loi contractuelle

Accords de licence transfrontaliers et licences de copies privés

Comme expliqué dans la stratégie européenne sur le *Cloud* Computing[47], les consommateurs devraient pouvoir utiliser de manière légale du contenu (acheté – couvert par le droit d'auteur) dans un/plusieurs Etats membres de l'UE sans perdre l'accès aux services pour lesquels ils ont payé dans n'importe quel autre Etat membre. La promotion de l'innovation par de tels accords de licence est importante vu les nouvelles sources de revenu que cela représente. La proposition de la Commission pour une directive sur la gestion collective des droits d'auteur[48] traitera, quand elle sera adoptée, beaucoup d'exigences relatives aux licences transfrontalières concernant le contenu du *cloud* dans le domaine de la musique. La Commission européenne est

[46] Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM/2012/010 final, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:EN:PDF.
[47] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Unleashing the Potential of Cloud Computing in Europe, COM(2012) 529 final, 27.9.2012.
[48] Proposition de directive du Parlement européen et du Conseil concernant la gestion collective des droits d'auteur et des droits voisins et la concession de licences multi territoriales de droits portant sur des œuvres musicales en vue de leur utilisation en ligne dans le marché intérieur, COM(2012) 372 final, 11.7.2012.

actuellement en train de rechercher d'autres mesures relatives au Livre vert[49], telles que la facilitation des licences pour la distribution en ligne d'œuvres audiovisuelles, en particulier à travers les frontières. Un service de *cloud* computing peut également permettre de sauvegarder du contenu dans le *cloud*. Le consommateur peut également utiliser le *cloud* comme un casier numérique pour son propre contenu et comme outil de synchronisation pour accéder à son contenu à partir de diverses machines. C'est pourquoi les questions relatives à la collection éventuelle de taxes pour les copies privées des œuvres qui sont dans ce contenu vers, de ou dans le *cloud* doivent être traitées en conséquence.

L'analyse des experts relative aux actions législatives possibles dans le domaine des redevances sur les copies privées dans l'UE est actuellement en cours, et est sous la direction de l'ancien commissaire européen de Justice et de l'Intérieur, Monsieur Antonio Vitorino[50]. Se basant sur les conclusions obtenues, la Commission évaluera le besoin de clarifier la délimitation de l'exception des copies privées et de la pertinence des redevances, en particulier à quel point les services de *cloud* computing permettant la rémunération directe des détenteurs de droits sont exclus du régime des redevances pour copies privées.

Conditions de contrat sûres et justes

Vu le cadre légal complexe relatif au *cloud* computing, les fournisseurs de *cloud* utilisent en général des contrats de niveaux de service (SLAs) complexes. Même si les contrats « à prendre ou à laisser » conviennent très bien aux fournisseurs, ce n'est pas le cas pour les utilisateurs du service, vu qu'ils n'ont que très peu de pouvoirs de négociation au niveau des modifications ou améliorations des contrats. Etablir des conditions de contrat standard qui sont sûres et justes sera donc très pratique afin d'offrir plus de protection aux consommateurs finaux du *cloud*.

Comme confirmé lors de la réunion avec les représentants du DG Connect, de telles conditions n'existent pas encore en ce moment mais on y travaille sur le terrain. Les conditions qui ont déjà été développées par le National Institute for Standards and Technology (NIST) américain sont actuellement étudiées. Un dialogue avec les parties impliquées est en cours afin de proposer des cas de référence/pratiques basés sur les résultats de cette consultation. La communauté de fournisseurs est très diverse; il est donc important de représenter les intérêts de tous les membres. Le processus de discussion est actuellement dans sa phase initiale et la coopération avec les autres services de la Commission européenne, dont la DG Justice, est important. Quant aux consommateurs et aux petites entreprises, la proposition de la Commission relative à un

[49] Livre vert sur la distribution en ligne d'œuvres audiovisuelles dans l'Union européenne - Vers un marché unique du numérique : possibilités et obstacles, COM(2011) 427.

[50] See Commission Communication "A Single Market for Intellectual Property Rights" COM(2011) 287 – Action 8 – which launched this mediation process in order to "explor[e] possible approaches with a view to harmonising the methodology used to impose levies [....]" and stated that a "concerted effort on all sides to resolve outstanding issues should lay the ground for comprehensive legislative action at EU level". The eCommerce Communication, COM(2011) 942 final, envisages a legislative initiative on private copying in 2013. The question on how the private copying exception applies to illegal content was equally addressed by the European Court of Justice as referred by the Austrian courts in Kino.to and the Dutch courts in ACI Adam B.V. v Stichting de Thuiskopie.

droit commun européen de la vente[51], prévoit des réponses claires à beaucoup d'incertitudes qui sont souvent créées par les stipulations nationales divergentes.

Il est évident que la création de *best practices* relatives aux conditions de contrat modèles accélérerait les processus *cloud* vu que cela renforcerait la confiance de clients potentiels. Une fois que les lignes directrices, validées au niveau de l'UE, seront reconnues par les autorités de contrôle des Etats membres, elles serviront de règles de conduite pratiques sur le terrain. Pour cela, il vaut la peine d'attirer l'attention sur les objectifs de la Commission pour l'année 2013, comme énumérés dans sa stratégie relative au *Cloud* Computing, au niveau des conditions contractuelles standard :

- Elaborer, avec les parties prenantes, des clauses contractuelles types pour les accords sur le niveau de service applicables aux contrats entre prestataires de services en nuage et utilisateurs professionnels, prenant en considération l'acquis en cours d'élaboration dans ce domaine ;
- Proposer, conformément à la communication relative au droit commun européen de la vente[52], des clauses et conditions contractuelles types aux particuliers et petites entreprises pour les aspects qui relèvent de la proposition en question; s'efforcer de normaliser les principales clauses et conditions d'un contrat, afin de dégager les meilleures pratiques en matière de clauses contractuelles pour les services en nuage en ce qui concerne les aspects liés à la fourniture de « contenu numérique » ;
- Charger un groupe d'experts créé à cette fin et comprenant des représentants du secteur de définir d'ici à la fin de 2013, pour les aspects qui ne relèvent pas du droit commun européen de la vente, des clauses et conditions contractuelles types sûres et équitables pour les particuliers et les petites entreprises sur la base d'un instrument facultatif de même type ;
- associer l'Europe à la dynamique de croissance mondiale de l'informatique en nuage en réexaminant les clauses contractuelles types applicables aux transferts de données personnelles vers des pays tiers en les adaptant, le cas échéant, aux services en nuage et en invitant les autorités nationales de protection des données à approuver des règles d'entreprise contraignantes spécifiques pour les prestataires de services en nuage[53];
- collaborer avec le secteur concerné à l'adoption d'un code de conduite destiné aux prestataires de services informatiques en nuage et favorisant une application uniforme des règles de protection des données, qui pourra être soumis pour approbation au groupe de travail « Article 29 » afin de garantir la sécurité juridique et la cohérence entre ce code de conduite et le droit de l'UE.

[51] Proposition de règlement du Parlement européen et du Conseil relatif à un droit commun européen de la vente, COM(2011) 635 final, 11.10.2011.
[52] Communication de la Commission «Un agenda du consommateur européen - Favoriser la confiance et la croissance», COM(2012) 225 final.
[53] Les avis pertinents du groupe de travail « Article 29 » (voir WP 195 et WP 153) serviront de base à ce projet de la Commission. Les règles d'entreprise contraignantes (BCR) constituent un des moyens de permettre les transferts internationaux légaux de données : elles contiennent des dispositions applicables à la manière dont les différentes entités d'une entreprise, où qu'elles soient établies dans le monde, traitent les données personnelles.

6.2.3 Le commerce électronique

L'instrument légal communautaire existant qui peut être appliqué sur le terrain est la directive sur le Commerce électronique[54]. Un des aspects les plus importants de la directive concerne la responsabilité intermédiaire, ce qui couvre la responsabilité du *cloud* provider pour les données qu'il « accueille ». Le but de ce régime consiste à garantir que les intermédiaires de données ou de contenu soient exonérés de responsabilité (par exemple, lors d'opérations faites dans le cadre des règles « Safe Harbor ») dans les cas où ils ne sont pas responsables des données ou du contenu en question. La directive fait une distinction entre les acteurs agissant comme « simple transport » (mere conduit), pour la forme de stockage dite « caching » et l'hébergement (« hosting »). Le fournisseur qui agit en tant que simple transporteur, transmettant des données ou du contenu à travers un réseau de communication, ne sera pas responsable pour autant qu'il n'initie / ne reçoive pas la transmission ou qu'il ne modifie pas son contenu. Quant au « caching », le fournisseur des services qui facilite la sauvegarde automatique, intermédiaire et temporaire de données ou de contenu, uniquement pour rendre la transmission du contenu plus efficace, il ne sera pas responsable de la nature du contenu pourvu que certaines conditions soient remplies. En dernier lieu, quant à l'hébergement, le fournisseur de service n'est pas responsable du contenu sauvegardé dans le cadre de ses services pourvu que certaines conditions soient remplies (p. ex. pas de connaissance de contenu illégal et action rapide pour supprimer le contenu illégal en cas de découverte).

Un autre domaine problématique relatif à la directive sur le Commerce électronique, semble être les procédures de notification et d'action. Les procédures de « notification-et-action » font référence à l'enlèvement ou au blocage d'accès au contenu illégal effectué par une entreprise en ligne, après que celle-ci ait reçu la demande de le faire. Afin de lui éviter la responsabilité, la directive sur le Commerce électronique oblige l'intermédiaire en ligne de passer à l'action dès qu'il est conscient du contenu illégal. Entrer en action peut se faire sous forme d'un démontage (supprimer le contenu litigieux) ou d'un blocage (bloquer l'accès au contenu litigieux).

La Commission a l'intention d'analyser les préoccupations des différentes parties concernées. Celles-ci concernent le fait que du contenu illégal en ligne existe de longue date et qu'il y a un manque de respect établi pour les droits des auteurs ou fournisseurs de contenu. L'analyse devra répondre à différentes questions : comment exactement un intermédiaire devrait-il être averti ? Cet avertissement ou notification devrait-il se faire de manière électronique ? La notification devrait-elle contenir une adresse internet détaillée ? Un détenteur de contenu « suspect » devrait-il avoir la possibilité d'être entendu et d'expliquer pourquoi il croit que ce contenu n'est pas illégal ? Si le contenu est effectivement illégal, en combien de temps un intermédiaire devrait-il agir ? Faut-il plus de transparence ou de publicité au niveau des procédures de notification et d'action entreprises individuellement par des personnes ou sociétés ?

[54] Directive 2000/31/Ce du Parlement européen et du Conseil, du 8 juin 2000, relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (« directive sur le commerce électronique ») JO L 178/1, 17.7.2000.

Certaines de ces questions sont relatives à la détermination de la législation qui est applicable (p.ex. : Où se trouve l'établissement, l'exploitation ?) ou à l'application des procédures de notification relatives au contenu ou aux activités (soi-disant) illégales de ces services émergeants (inclus le *cloud* computing). Ces questions ont été traitées dans la communication sur le marché unique numérique du commerce électronique et des services en ligne, dans l'approche de la Commission au niveau des procédures de notification et d'action[55].

6.2.4 Standards et certification

Comme indiqué dans la stratégie européenne sur le *Cloud* Computing[56], une utilisation plus étendue des normes (standards), la certification des services de *cloud* afin de démontrer qu'ils répondent à ces normes et la validation de cette certification par les autorités régulatrices comme évidence du respect des obligations légales aideront l'industrie du *cloud* à décoller. La Commission européenne a donc l'intention d'introduire des normes européennes relatives au *cloud* computing ; ainsi que de créer une liste des fournisseurs de *cloud* computing fiables.

Les normes ou standards

La normalisation du *cloud* influencera également les parties intéressées bien au-delà de l'industrie informatique, en particulier les PME, les utilisateurs du secteur public et les consommateurs. Les PME en particulier sont rarement capables d'évaluer les revendications des fournisseurs quant à leur implémentation de standards, l'interopérabilité de leurs offres *cloud* ou la facilité avec laquelle les données peuvent être migrées d'un provider à un autre. C'est la raison pour laquelle une certification indépendante et crédible s'impose.

Des actions de standardisation dans le domaine du *cloud* computing sont déjà en place. Le « National Institute for Standards and Technology » (NIST) américain a publié une série de documents, dont un ensemble de définitions qui sont largement acceptées. L'Institut européen des normes de télécommunication (*ETSI*) a fondé un groupe de réflexion sur les besoins et la conformité au niveau des normes d'interopérabilité. A l'ETSI, la première réunion de coordination relative aux normes de *cloud* a eu lieu les 4 et 5 décembre 2012 à Cannes. Trois sujets principaux ont été traités :

- Normes relatives aux SLA ;
- Normes relatives à la sécurité ;
- Normes relatives à l'interopérabilité, à la portabilité des données et à la réversibilité.

Comme expliqué à l'équipe d'étude par les représentants de la DG Connect, l'exercice de recensement des matières à traiter a été accompli ; ses résultats seront sans doute disponibles avant l'été 2013. Le but principal ne consiste pas à définir des normes nouvelles mais à étudier les spécifications techniques existantes étant donné que l'ETSI

55 Communication de la Commission au Parlement européen, au Conseil, au Comite économique et social européen et au Comité des régions : « Un cadre cohérent pour renforcer la confiance dans le marché unique numérique du commerce électronique et des services en ligne », COM(2011) 942 final, 11.1.2012, p. 15
56 http://ec.europa.eu/information_society/activities/cloudcomputing/docs/com/com_cloud.pdf

a déjà réalisé beaucoup de travail dans ce domaine. La cartographie des normes n'est encore que dans une phase initiale et donc aucune décision n'a été prise jusqu'à présent. On prévoit néanmoins que la Commission continuera son travail en collaboration avec l'ETSI, l'ENISA et d'autres organisations compétentes afin d'assister au développement de schémas de standardisation européens dans le domaine du *cloud* computing (dont la protection de données).

Certification

La question de la certification pour les fournisseurs de *cloud* est aussi importante que l'assurance de sécurité, ces deux aspects étant également critiques pour le développement du *cloud* computing. La Commission européenne ne planifie cependant pas la mise en place de certifications spécifiques, ce qui démontre son approche prudente dans la matière (en partie expliquée par le risque de coûts élevés d'une telle certification). Pour la Commission, la décision est à prendre par les opérateurs du *cloud* eux-mêmes.

La Commission est néanmoins en train d'explorer l'utilité et les avantages des systèmes de labels de confiance européens – connus dans l'Action 17 de l'Agenda numérique pour l'Europe (Digital Agenda). Le travail dans ce domaine est basé sur la collaboration avec l'ENISA. On connaît dans ce domaine divers signes ou labels de qualité comme le « petit cadenas jaune https » en matière de sécurité ou les labels d'accessibilité des sites Web définis par le W3C. Ce sujet est considéré comme important car la mise en place des garanties ou fonctionnalités que sous-entend et représente le label permet effectivement aux acteurs de renforcer leur confiance quant à la qualité du service. Cependant, il y a également quelques aspects négatifs, tels que les coûts que cela implique, ainsi que la difficulté de reconnaître les labels de confiance différents. La Commission n'a pas encore pris de position à ce sujet mais on en prévoit une bientôt, qui influencera considérablement la politique générale dans le domaine du *cloud* computing. Des problèmes fondamentaux devront être abordés ; une des solutions consisterait cependant à confier cette tâche à une agence européenne.

6.2.5 Le partenariat européen pour le c*loud*

Le partenariat européen pour le *cloud* (European *Cloud* Partnership ou ECP) a été fondé dans le cadre de la European *Cloud* Strategy et a pour but de réunir l'industrie et le secteur public afin d'établir un marché numérique unique pour le *cloud* computing dans l'Europe.

L'agenda de l'ECP comprend :

1) Le travail d'un comité de direction récemment formé : il comprend des représentants des autorités publiques et de représentants de l'industrie, son intention est d'offrir des conseils, de la coopération et de la stimulation pour le modelage du marché des services de *cloud* computing. Il n'y a pas de prise de position formelle si ce groupe sera élargi ou non.

2) Des activités préliminaires concernant un marché public : un appel d'offre relatif à la définition d'un environnement de *cloud* computing de haute qualité

correspondant aux besoins du secteur public a été publié (procédure clôturée le 15 janvier 2013). Le but est d'établir un forum d'échange d'idées et d'expériences entre les Etats membres afin de trouver les meilleures solutions *cloud* pour le secteur public et de faire remonter les expériences nationales à un niveau européen. Les premiers partenariats entre Etats membres pourront alors être établis ; ensuite le secteur privé dans les Etats membres pourrait être impliqué par le biais d'appels d'offre.

La critique que l'on peut formuler par rapport à cet environnement est qu'il reste encore assez flou, ce qui laisse certains Etats membres en proie à des tentations de *cloud* souverain, soit pour favoriser leur propre industrie de service, soit pour se prévaloir d'une meilleure protection contre les fuites d'information (par exemple, dans le cas particulier de pays qui ont une forte tradition de secret bancaire).

Dans sa communication stratégique[57], la Commission a clairement affirmé qu'elle ne souhaitait pas prendre la tête de la construction d'un « Super *Cloud* européen » dédié au secteur public. Elle n'exclut pas qu'un Etat puisse construire un *cloud* dédié (privé) pour le traitement de données sensibles, mais cela doit rester l'exception, la règle étant la mise en concurrence sur base d'un cahier des charges reprenant les exigences de qualité formulées par le secteur public.

Les initiatives purement nationales[58] sont critiquées à mots couverts parce que « *quand on fragmente ainsi le marché du secteur public, l'expression des spécifications (ou cahier des charges) a peu d'impact, le degré d'intégration des services est bas et les citoyens n'obtiennent pas la meilleure valeur pour leur argent* [59]». La voie qu'il est actuellement possible de suivre serait donc celle de la mutualisation (« *pooling public requirements* ») dans le cadre de collaborations ponctuelles ou sectorielles (santé, assistance sociale, services d'e-Gouvernement, données ouvertes), entre Etats ou services entrepreneurs. Au-delà de toute la complexité de mise en place de ces accords multipolaires pour « investir ensemble » (sur quel budget ? qui prendra la direction ? cela conduira-t-il à des partenariats ouverts à de nouveaux adhérents dans le cadre d'une Europe à plusieurs vitesses ?)[60], la première étape – qui est la tâche de l'ECP – est bien d'établir ces spécifications communes.

6.2.6 Etudes en cours relatives au c*loud* computing

Comme annoncé lors de la réunion avec les représentants de la Commission, deux études en cours sur le *cloud* computing doivent être prises en considération :

[57] COM (2012) 529 « Unleashing the Potential of Cloud Computing in Europe » – 27/9/2012 – p.6.
[58] Andromède en France, G-Cloud au Royaume-Uni, Trusted Cloud en Allemagne,…
[59] COM (2012) 529 – p. 13.
[60] On a vu dans la stratégie « *Pooling open source software* » initiée par la Commission dès 2002, combien – malgré la mise en place des plateformes OSOR.eu (2008) et plus récemment Joinup.eu (2012), et malgré les déclarations ministérielles UE de Manchester (2005) et Malmö (2009) - les initiatives restent soit communautaires, soit nationales, mais n'ont pas débouché sur une mutualisation intergouvernementale ou interrégionale.

1) L'étude sur les initiatives des Etats membres relatives à l'implémentation de *cloud* computing (réalisée par E-data). Sept Etats membres sont couverts et il est prévu que l'étude soit finalisée en juillet 2013.
2) L'étude visant à donner un aperçu plus général du travail d'implémentation dans le domaine du *cloud* computing réalisé par IDC.

7 Recommandations

7.1.1 S'inscrire dans l'approche européenne

Suivre l'avancement des projets (ne pas essayer de les devancer) :

- Le projet de règlement général sur la protection des données (le projet n'est pas encore figé). Il faut en particulier suivre les efforts de certains lobbyistes qui se servent de divers leviers, en particulier certains parlementaires européens, pour en modifier ou atténuer la portée[61] ;
- Les droits du consommateur qui souhaiterait confier au cloud des copies d'œuvres couvertes par des restrictions provenant de l'exercice du droit d'auteur ;
- L'évolution de la directive sur le commerce électronique ;
- Les standards techniques qui seront recommandés ou imposés par l'ETSI ou l'ENISA ;
- La participation au « partenariat européen pour le cloud ».

Dans tous ces domaines, il convient, non de légiférer de manière hâtive ou isolée, mais d'exercer une veille technologique et juridique afin de prévoir les réformes à venir et d'être en mesure de formuler des avis pertinents.
Cette acquisition de connaissance devrait permettre aux autorités publiques de jouer un rôle plus actif et visible dans l'ECP.

Comme option alternative, il est recommandé de travailler sur la promotion de bonnes pratiques qui préparent l'entrée en vigueur des réformes.

L'avantage est que ces « bonnes pratiques » peuvent être définies dans des documents de travail, par versions successives permettant de suivre avec souplesse l'actualité (version 1.0 – 2013 ; version 1.2 – 2014 etc.) et permettant aux acteurs intéressés de déclarer leur conformité à un niveau déterminé de ces « bonnes pratiques », sans qu'il soit besoin de mettre en place des procédures de certification rigides et coûteuses.

En ce qui concerne les besoins du secteur public, un état fortement régionalisé comme la Belgique ne devrait pas se concentrer sur la construction d'un « *cloud* souverain » qui équivaudrait à reconstruire des frontières économiques (nationales ou régionales) pour l'activité du *cloud*. Au contraire, il faut être attentif aux opportunités de développer des partenariats ouverts (à de nouvelles adhésions) avec les Etats voisins. En particulier, la mutualisation de certains appels d'offres (quand le cahier des charges du « *cloud* public » aura été défini dans le cadre du partenariat européen) et le partage de ressources en mode ouvert (principalement les applications logicielles spécialement développées par ou

[61] Voir à ce sujet la dénonciation par l'éditorialiste Glynn Moody des demandes d'amendement introduites par des parlementaires européens, qui reproduisent mot pour mot les desiderata de certaines firmes étrangères: « EU Data Protection: Proposed Amendments Written by US Lobbyists » dans : http://blogs.computerworlduk.com/open-enterprise/2013/02/eu-data-protection-proposed-amendments-written-by-us-lobbyists/index.htm.

pour le secteur public, dans divers Etats membres, en mode « open source » et suivant des standards ouverts et libres de droits) sont deux approches à privilégier, en coopération avec le Service public fédéral Technologie de l'Information et de la Communication (FEDICT).

7.1.2 Renforcer le dialogue avec et entre les acteurs économiques

Il y a eu un premier essai de former un groupe « Belgian *Cloud* ». La plupart des membres de ce groupe sont à présent actifs au sein de « BELTUG », une ASBL se voulant la plus grande organisation représentative des managers ICT, avec une préoccupation particulière pour les réseaux inter-entreprises, les communications mobiles, les « groupes d'amélioration du logiciel » (Software Improvement Group) concernant les communications unifiées et le c*loud*.

L'amélioration du *cloud* computing en Belgique et le renforcement de l'attractivité économique de ce secteur ne se fera pas par décret unilatéral de l'autorité publique, mais par la recherche des meilleures pratiques et par l'amélioration de la sécurité avec les acteurs concernés. Il est donc utile (que cela soit au sein de BELTUG ou autrement) de mettre en place un dialogue entre l'autorité publique et les professionnels de ce secteur, dans le but d'en améliorer l'attractivité et la confiance du marché.

Il serait bon que l'organisation de la profession des fournisseurs de c*loud* soit plus spécifiquement organisée, afin qu'ils jouent un rôle de référence ou d'avant-garde dans la bonne gestion de l'ICT pour les entreprises et les administrations publiques performantes et puissent fournir un interlocuteur dans le cadre des initiatives nationales et européennes. Il n'est pas évident que la structure régionale et linguistique de la Belgique soit un avantage pour la mise en place de cet interlocuteur. Il semble donc utile de se pencher sur cette question.

7.1.3 En matière contractuelle

Compte tenu des bonnes pratiques déjà établies, comme la décision 2002/16/CE de la Commission du 27 décembre 2001 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers en vertu de la directive 95/46/CE[62], compte tenu des BCR (Binding Corporate Rules[63]) considérées comme offrant des garanties suffisantes de protection des données grâce à des règles d'entreprise contraignantes, compte tenu aussi des observations de ce rapport et d'une check-list (voir section 8), il serait utile d'élaborer, de concert avec les représentants de la profession, un ou plusieurs contrats-types correspondants aux principaux modèles de service. Ces contrats pourraient reprendre les recommandations faites per le groupe de travail « Article 29 » (voir la liste des clauses contractuelles sous 6.2.1) et ainsi devancer (et tenir compte) de l'orientation du projet de règlement général

[62] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:006:0052:0062:FR:PDF.
[63] Une BCR est une règle élaborée par une entreprise multinationale (tel un code de conduite interne), qui doit être obligatoire pour l'ensemble de ses entités et employés, et qui porte sur les transferts internationaux de données personnelles réalisés au sein du groupe.
http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/index_en.htm.

de protection des données et servir de standards de qualité et de référence, tout en renforçant la confiance du marché des entreprises et des administrations publiques.

Dans la mesure où l'investissement reste limité et où cela pourrait être repris et adopté par d'autres partenaires européens, l'adhésion – volontaire – à ces spécifications contractuelles pourrait se voir récompensée par l'attribution d'un label « ***Fair Cloud*** » (à dessiner) et par la publication par l'autorité régulatrice d'une liste des adhérents à ces spécifications. La publicité donnée à ce label renforcera la confiance et l'attractivité du marché.

7.1.4 En matière d'information du public

Publication d'un guide pratique
Certains pays[64] ont publié de petits guides pratiques à l'attention des entreprises et des citoyens. Un tel document ne doit pas être long (20 pages au maximum) et être d'une lecture facile.

On devrait y trouver :

- un aperçu du *cloud* : des notions, modèles de déploiement et de service ;
- une définition des rôles et des responsabilités qui s'y rattachent ;
- des recommandations pratiques sur l'adoption du *cloud* (comment choisir et évaluer son fournisseur, que considérer dans son contrat) ;
- quelles sont les règles internes à adopter par le client du *cloud* et la formation de base qu'il doit acquérir pour garder le contrôle et gérer son fournisseur (et non être géré par lui) ;
- une « check list » (voir ci-dessous) ;
- des illustrations pratiques qui se réfèrent à la réalité quotidienne ;
- une liste « qui fait quoi ? » qui donne au candidat utilisateur des points de contact auprès des représentants de la profession et auprès de l'autorité publique, surtout dans la mesure où celle-ci peut assurer une mission de guidance, de contrôle ou de conciliation.

Il semble utile de prendre exemple sur ce qui existe et de publier un tel guide, dans au moins les trois langues nationales et l'anglais afin que ce guide serve de « carte de visite » du *cloud* en Belgique, à l'attention des entreprises, des administrations et des clients potentiels en Belgique et à l'étranger.

[64] Voir : UK – (Information Commissioner's Office) « Guidance on the Use of Cloud Computing – 2 October 2012; Ireland – NSAI Standards, SWiFT 10:2012 "Adopting the Cloud – decision support for cloud computing"; Slovenia – Information Commissioner and Cloud security alliance, Slovenia chapter – "Personal data protection and cloud computing (15 Juin 2012).

Comment illustrer le guide au moyen de cas pratiques ?

Exemple :
Une école envisage de moderniser ses méthodes d'enseignement par la création de « classes informatiques » ou chacun à son poste de travail.
Traditionnellement, cela impliquerait l'achat de PC indépendants pour chacun (de payer des licences par poste, de gérer la sécurité, les anti-virus, les accès internet, les déchargements ou chargements dont les élèves prendraient l'initiative, la maintenance, etc., pour chaque poste). En optant au contraire pour l'accès à une solution *cloud* spécialisée (SaaS), l'école évitera tous ces problèmes et les postes (par exemple des tablettes) n'opéreront que dans le cadre prévu.
La solution permet aux étudiants d'accéder à leurs travaux à partir de n'importe quel point (école, maison) et de suivre leurs performances (résultats).

L'école qui met en place le service est le client du c*loud*. L'école est aussi le « responsable du traitement » qui doit demander la mise en place d'une protection des données personnelles (les noms, l'accès aux appréciations des professeurs).

Le fournisseur de *cloud* est le « processeur » du traitement (le sous-traitant selon la loi) mais, en tant que professionnel, il doit conseiller l'école et lui fournir une application qui réponde aux critères de sécurité attendus (contrôle d'accès, vérification de l'identité, cryptage) et veiller à ce que le contrat de niveau de services précise les lieux de stockage, la disponibilité du service, les procédures de rectification et d'effacement des données, le fait que les données ne peuvent être utilisées à de fins commerciales, etc.

L'étudiant est le sujet des données (la « personne concernée ») qui a le droit de connaître les données qui le concerne et le droit d'en demander rectification en cas d'erreur.

Publication d'une check list.
L'idée de publier une « check list » du *cloud* computing avait été particulièrement bien accueillie lors de la réunion qui s'est tenue le 27 février 2013 avec les opérateurs du *cloud*.

La check list pourrait contenir des points relatifs :

- Au client lui-même (qui doit se connaître, savoir s'il traite des données à caractère personnel, savoir quels sont ses besoins et exigences en matière de trafic, de continuité d'affaires, de support etc.) ;
- Au fournisseur de cloud ;
- Aux relations contractuelles entre le client et son fournisseur.

Une tentative de check list est donnée dans la section 8.

7.1.5 En matière de sécurité

Le caractère critique des infrastructures de c*loud* doit pousser les autorités publiques à :

1) Conduire sur le terrain, de manière pratique et réaliste, une évaluation des risques (tels qu'ils sont relatés à la section 4 de ce rapport) qui menacent le *cloud*, par ordre

de priorité et en particulier pour les services IaaS et PaaS implémentés sur notre territoire.
Pour éviter de se disperser, il faut d'abord se concentrer sur les services dont l'indisponibilité pourrait impacter de nombreuses autres organisations :

- Identifier ces grandes infrastructures ou plateformes sur base du degré de dépendance de l'activité économique par rapport à celles-ci, et dresser une carte de ces dépendances physiques et logiques ;
- Analyser ce qui est vital pour ces infrastructures, non seulement leur protection physique, mais également leur alimentation en énergie, leur refroidissement, leur accès aux réseaux de communication.

2) Identifier et faire adopter (en vérifiant qu'elles soient effectivement adoptées) les mesures de sécurité recommandées, soit pour prévenir les incidents, soit pour limiter leur impact. Veiller en particulier à éviter qu'il y ait, en tous les endroits physiques ou logiques (software) de la chaîne de production, des « points faibles uniques » (single points of failure) et que la redondance fasse que la mise hors service d'un système puisse être compensée par d'autres.
Que cela soit ou non dans le cadre d'une certification, la promotion et l'exigence d'audits réguliers, de préférence indépendants, est ici particulièrement recommandable : ceci doit être confié à des professionnels qui suivent de près l'évolution des risques. Dans le domaine très évolutif de la sécurité, plutôt que d'opter pour une périodicité « automatique » (par exemple annuelle), il faudrait pouvoir inviter les acteurs du *cloud* à se mettre en conformité et exercer éventuellement le contrôle « dès que nécessaire » quand il apparaît qu'une mesure doit être mise en place. Dans ce cadre, l'autorité devrait mettre en place, en coopération avec les représentants du secteur, une cellule d'observation afin de détecter quelles mesures recommander (ou le cas échéant imposer) et dans quelles limites (en fonction de l'importance du service).

3) Obtenir de manière systématique un rapport sur tous les incidents survenus soit en matière de sécurité, soit en matière d'interruption de service (au-delà d'une limite à fixer), de manière à valider l'évaluation des risques. Quand l'incident porte sur la sécurité, une attention particulière devrait être portée à l'échange de ces informations entre les diverses autorités ou gouvernements concernés, en tirant profit des outils développés à cette fin par l'Union européenne (comme le réseau CIWIN). Le rôle des pouvoirs publics est ici de promouvoir une culture d'échanges d'information entre tous les acteurs concernés, de manière à faciliter une adoption rapide des mesures appropriées (alors que les technologies évoluent rapidement).
Il faut aussi, en coopération avec les représentants de la profession, définir à partir de quand et dans quelles limites il doit être obligatoire de rapporter un incident.
Quand un incident peut donner lieu à des poursuites ou à des sanctions, il faut que le fait de rapporter volontairement un incident réduise fortement, voire immunise la responsabilité du rapporteur (au moins en matière de sanction pénale, de même que les sociétés qui signalent un cartel ou une distorsion de concurrence à l'autorité européenne peuvent échapper aux sanctions).

4) Utiliser le travail d'information (voir section précédente) en communiquant aux entreprises et au public qu'un effort particulier est fait pour renforcer la sécurité du

cloud, notamment le fait que les rapports d'incidents sont systématiquement collectés, que les risques sont analysés et que les mesures prises pour les prévenir et réduire les conséquences des problèmes sont effectivement identifiées et suivies.

Ce « triangle de gouvernance » peut être mis en place de manière privée par une association professionnelle, mais il faut dans ce cas que le régulateur (l'autorité publique) joue son rôle de contrôle en étant informé des rapports, de tout événement survenu et du suivi des mesures prises.

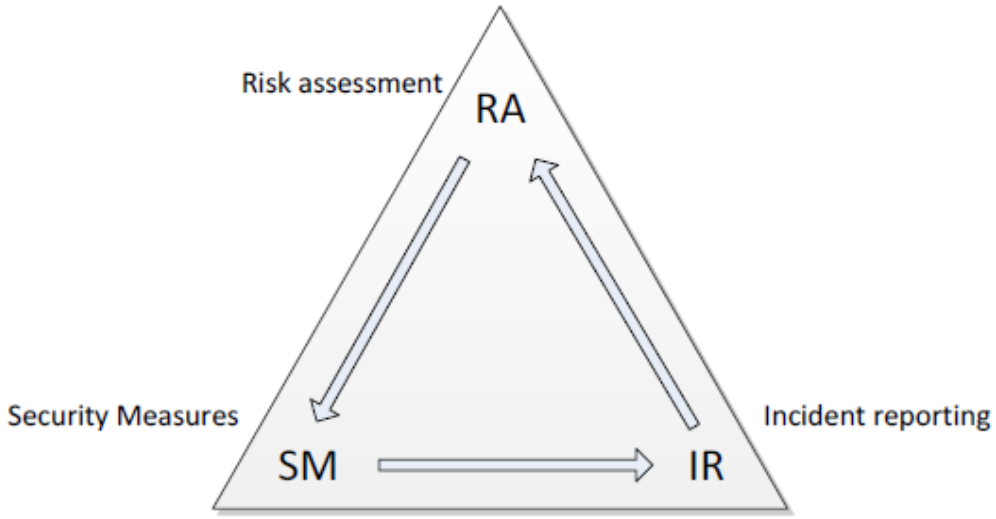

Figure 11 - Combiner l'évaluation des risques (RA), la mise en place de mesures (SM) et le rapport des incidents (IR) (source : Rapport ENISA, décembre 2012)

Quand on parle d'autorité de contrôle, qui désigne-t-on ? Dans les recommandations de l'ENISA de 2012, ce sont les agences responsables pour établir et entretenir les plans nationaux de limitation des risques (« Agencies responsible for establishing and maintaining national contingency plans »)[65]. Dans la mesure où les service *cloud* sont reconnus comme critiques, c'est-à-dire « *installation, système ou partie de celui-ci, d'intérêt fédéral, qui est indispensable au maintien des fonctions vitales de la société, de la santé, de la sûreté, de la sécurité et du bien-être économique ou social des citoyens, et dont l'interruption du fonctionnement ou la destruction aurait une incidence significative du fait de la défaillance de ces fonctions* », on peut faire référence à la Direction générale Centre de Crise du Service public fédéral Intérieur (DGCC) désignée par la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques pour analyser et contrôler la mise en place de ces protections et le travail des acteurs concernés et faire appliquer les mesures prévues par cette loi.

[65] ENISA, Critical Cloud Computing – a CIIP perspective on cloud computing services – December 2012 [Online] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/critical-cloud-computing, p. 23.

8 Check list

Parmi les recommandations les mieux accueillies (lors du meeting avec les acteurs du *cloud*) figure la publication d'une « check list » qui aiderait le client du *cloud* à identifier ses propres besoins et à choisir son fournisseur en pleine connaissance de cause.

Nous formulons ci-après un avant-projet :

Votre position (comme **responsable du traitement** selon la LPV) en tant que « Client » du *cloud* (examen interne)	Quels sont les bénéfices commerciaux ou économiques que vous attendez du *cloud* ? - Avez-vous compris le modèle économique proposé ? - Avez-vous évalué (par ex. sur 5 ans) les coûts opérationnels par rapport aux investissements en capital ? - Avez-vous considéré la bande passante nécessaire et son coût ?	
	Quels sont les autres bénéfices que vous attendez du *cloud* ? Quel est l'impact attendu sur : - Votre organisation (organigramme, rôles) - Votre niveau de connaissance (formations) - Vos processus - Votre facilité de maintenance	
	Comment voyez-vous l'évolution de votre « consommation informatique » durant les 5 prochaines années, selon que la croissance se fait en interne ou à l'extérieur (ressources du *cloud*) ?	
	Vos données contiennent-elles des données à caractère personnel (toute information, même un simple numéro qui peut désigner de manière unique une personne physique identifiée ou identifiable et se rattacher à elle)? Si oui, en faites-vous soigneusement la liste ?	LVP 1, §1
	En qualité de « contrôleur » de ces données (ou « **responsable du traitement** de données à caractère personnel » selon la LVP) et de futur « client » d'un service *cloud*, avez-vous la base légale requise pour traiter ces données ?	LVP 4 & 5
	Avez-vous vérifié qu'aucune de ces données n'est « interdite » ou limitée (race, opinion, santé, etc.) ou que vous bénéficiez dans ce cas d'une des exceptions prévue par la loi ?	LVP 6, 7 & 8

	Avez-vous déterminé quelles données (y compris celles ci-dessus) dont vous êtes le contrôleur, donc le responsable du traitement, vont être traitées dans le *cloud* ?	
	Avez-vous vérifié qu'aucune autre disposition (par exemple contractuelle) ne limite le traitement de ces données (si elles se rapportent à vos propres clients, à vos membres etc.) ?	
Votre fournisseur	Depuis combien de temps votre fournisseur est-il actif dans le *cloud* ? Communique-t-il une liste de références ? Avez-vous accès à ses comptes publiés (ou à un audit économique le concernant) ?	
	Votre fournisseur est-il couvert par une assurance qui couvre aussi vos données et la perte d'affaires en cas d'indisponibilité, et le cas échéant un arrangement « escrow » ou autre qui vous garantisse de recouvrer vos données ?	
	Votre fournisseur est-il (ou fait-il partie d'un groupe, y compris ses centres de traitement de données et sous-traitants) établi exclusivement sur le territoire de l'Espace économique européen (Union européenne, Norvège, Islande, Liechtenstein) ?	
	Si votre fournisseur a des établissements ou utilise des centres de traitement « hors EEE », les pays où ces établissements ou centres sont situés sont-ils repris dans la liste publiée par la Commission européenne comme « offrant un niveau de protection des données suffisant » ?	
	Si votre fournisseur utilise des établissements ou centre de traitements en dehors de l'EEE (principalement les Etats-Unis), est-il globalement certifié comme appliquant les principes définis dans l'accord « Safe Harbor » ?	
	Votre fournisseur vous a-t-il proposé un contrat de service (obligatoire pour les données à caractère personnel) qui définit sa responsabilité et mentionne les garanties qu'il offre en matière de sécurité et d'organisation ?	LVP 16 §1, 1°-4°
	Ce contrat avec le fournisseur de *cloud* est-il écrit (obligatoire pour les données à caractère personnel), étant entendu que cet écrit peut être sous forme électronique ?	LVP 16 §1, 2° & 5°
	S'il y a des données à caractère personnel, le fait que le fournisseur de *cloud* en est responsable vis-à-vis de vous et accepte d'être tenu par les mêmes obligations que vous (responsable du traitement) sont-ils expressément mentionnés dans le contrat ?	LVP 16 §1, 5°
	Votre fournisseur de c*loud* a-t-il fait auditer sa sécurité par un expert indépendant, et les conclusions de ce rapport vous ont-elles été communiquées ?	

Les dispositions de votre contrat	Les mesures en place au terme de ce rapport correspondent-elles (ou dépassent-elles) au cahier des charges ou à une norme de qualité que vous considérez comme appropriée dans votre secteur d'activité ?	
	Dans quel délai votre fournisseur s'engage-t-il à vous informer au cas où il a pu constater un défaut de sécurité dans les services ou produits qu'il propose ?	
	Comment pouvez-vous gérer la création de nouveaux comptes d'utilisateur ? Quels sont les délais opérationnels (et le coût éventuel) pour la création, la suspension, la suppression d'un compte ?	
	Cryptage : Est-il garanti que les données soient encryptées en cas de transit à l'intérieur du « *cloud* » (par exemple entre deux centres de traitement géographiquement distincts) ? Est-il garanti (si nécessaire, pour des données personnelles) que les données soient encryptées quand elles sont « au repos » dans le serveur *cloud* proposé ? Le système de gestion (génération / conservation) des clés de cryptage est-il mis en place ?	
	Au cas où vous demandez la destruction définitive de certains enregistrements ou données, est-ce que votre fournisseur vous garantit leur destruction effective (écrasement/remise à blanc) dans toutes les copies ou versions qui pourraient être conservées sur le *cloud* ? Quel est le délai pour que cette destruction ait lieu ?	
	Au cas où vous décidez de mettre fin aux services *cloud*, est-ce que votre fournisseur vous garantit la destruction effective (écrasement/remise à blanc) de toutes copies ou versions de ces données qui pourraient être conservées sur le *cloud* ?	
	Avez-vous identifié tous les cas où vos données (y compris des informations au sujet de vos utilisateurs) pourraient être ou non partagées ou communiquées avec d'autres parties (relations, « amis », etc.) ou utilisées dans le cadre d'autres services que le fournisseur de *cloud* pourrait offrir (par ex. offres commerciales, e-mailing) ?	
	Le fournisseur vous donne-t-il un moyen d'être informé et de contrôler la liste de qui a eu accès, à quelles de vos données, et quand ?	
	Le fournisseur vous garantit-il de pouvoir obtenir sur demande et sans conditions une copie de vos données, dans un format utilisable (conforme à un standard ouvert, libre de droits, largement utilisé et bien documenté) pour le transfert éventuel de ces données à un autre fournisseur ?	

	En cas de panne ou de destruction imprévue (par exemple le bris d'un disque), quel est le délai garanti pour une remise en route / une restauration sans altérations depuis une copie de sauvegarde ?	
	Le fournisseur peut-il garantir que son service a une capacité suffisante pour maintenir votre qualité de service en cas de « pics d'utilisation » provoqués par d'autres utilisateurs ?	
	A quel point les opérations de ces autres utilisateurs peuvent-elles dégrader la qualité des services qui vous sont dus ?	
	Y a-t-il un engagement du fournisseur de vous assurer en permanence l'accès à son service ou à vos données ? Quelle est la tolérance (période d'interruption maximum tolérable), compte tenu de votre activité ?	
	Avez-vous fait l'estimation des coûts de matériel (postes périphériques, routeurs) et de connexion (abonnements) de tous vos utilisateurs, quand ils accèderont aux services *cloud* 1) depuis leur bureau habituel 2) hors du bureau habituel (au domicile ou en voyage) ?	
	Les droits et obligations des parties (votre fournisseur et vous-même) sont-ils décrits en détail dans un contrat écrit ? (une convention de niveau de service ou SLA – « Service Level Agreement »)	
	Votre fournisseur s'est-il engagé à vous communiquer tout changement (dans ses conditions, son fonctionnement, son infrastructure, ses services) qui pourrait avoir une influence sur l'exécution de votre contrat avec lui ?	
	Le contrat limite-t-il la liste des pays où vos données peuvent être transférées, stockées ou traitées (par exemple, uniquement les pays de l'Union européenne, ou de l'Espace économique européen) ?	
	Dans d'autres cas, ces pays où les données peuvent être transférées présentent-ils des garanties suffisantes selon la Commission européenne, c'est-à-dire : Canada, Suisse, Argentine, Guernesey, île de Man, îles Féroé, Jersey ou Israël (pour les Etats-Unis, voir ci-dessous) ?	
	Si les Etats-Unis font partie des pays où les données peuvent être transférées, tous les destinataires (centres de traitement *cloud,* filiales ou contractants) ont-ils formellement adhéré aux principes de l'accord UE-US « Safe Harbor ») ?	

	Si le fournisseur de *cloud* entend utiliser une infrastructure répartie sur d'autres pays tiers (autres que les pays d'Europe /EEE ou présentant des garanties suffisantes), quelles sont les garanties en matière de protection des données et ces garanties – sous forme de contrat ou contrat-type - et ont-elles été autorisées par un arrêté royal après avis de la Commission de la protection de la vie privée ?	
	Le fournisseur peut-il documenter dans quelles circonstances et pourquoi vos données pourraient être transférées dans d'autres pays ?	
	De manière générale, avez-vous la possibilité préalable de vous opposer à un transfert de données ou de le limiter aux données ou aux pays que vous jugeriez appropriés ?	

9 Clauses contractuelles de référence

Il est assez difficile d'élaborer un contrat-type tant les situations, les attentes des clients, leurs propres modèles d'activité et le prix qu'ils sont prêts à payer pour le service (OPEX vs CAPEX) sont différents. A défaut d'une offre de type « public » très standard, c'est-à-dire limitée à des fonctionnalités bien précises, ces questions de prix, ainsi que beaucoup d'autres relatives aux références du fournisseur (ses autres clients, y compris les contrats clôturés « à la satisfaction des deux parties »), le détail des services et des fonctionnalités offertes, la capacité de croissance des services (sur x années) ne peuvent être réglées que dans la liste des points à vérifier (check list), un SLA individualisé ou dans des annexes.

Les idées de clause données ci-après pourraient toutefois, suivant accord avec un groupe représentatif de la profession être adoptées comme correspondant à un label « ***Fair Cloud*** »

Intitulé	**Clause**	**Remarque**
Définitions	Le client du cloud (/ nuage) est la personne qui fait appel au fournisseur de cloud (/ nuage) pour utiliser, à distance, sur demande et par l'intermédiaire d'un réseau de télécommunication, des ressources informatiques qui lui permettent d'exercer son activité et de traiter ses données. Le fournisseur du cloud (/ nuage) est la personne qui propose au client, à titre gratuit ou onéreux, une infrastructure (des capacités), une plateforme opérationnelle et/ou des applications permettant au client de charger, traiter et conserver ses données.	Nécessité de définitions de rôles qui peuvent se rattacher à la législation applicable
Attentes du client et niveau de service	La nature des services, les demandes spécifiées par le client et le niveau de service attendu sont précisés de manière objective et mesurable dans l'annexe 1. Il est prévu des pénalités pour compenser le dommage au cas où le fournisseur n'assurerait pas le niveau de services prévu. Ces pénalités sont fixées de manière objectives et mesurables en annexe 2.	
Durée des services	La durée du service (période couverte) ainsi que la possibilité de renouveler ou de mettre fin aux services est fixée en annexe 3.	
Continuité des affaires / Contrat de niveau de services	Le fournisseur garantit une disponibilité du service de __ % et un redémarrage en cas d'interruption après incident dans un délai maximum de _ heures, fixés dans le contrat de niveau de service.	
Assurance professionnelle	En plus des pénalités forfaitaires prévues si le niveau de qualité du service n'est pas atteint, le fournisseur a contracté une assurance professionnelle afin d'indemniser le dommage réel direct et indirect subi par le client (en cas d'interruption d'activité,	

	perte d'affaires, dommages à l'image etc.). Ce montant assuré est plafonné par sinistre à X.	
Nature des données traitées (1)	Au cas où les données sont à caractère personnel (au sens de la directive 95/46 CE), le client déclare qu'il est – en sa qualité de « responsable du traitement » dans les conditions légales pour les charger et les traiter.	Rattachement au droit en vigueur
Nature des données traitées (2)	En annexe 4, le client mentionne si les données qu'il met sur le cloud sont « à caractère personnel » et décrit brièvement quelles sont ces données et le but du traitement. A défaut de cette déclaration formelle, et si le fournisseur n'a pas pris l'engagement de traiter TOUTES les données du client COMME SI elles étaient à caractère personnel, le fournisseur est en droit de supposer que les données n'ont aucun caractère personnel.	Protection simple ou renforcée
Nature des données traitées (3)	Au cas où le fournisseur accepte d'héberger des données à caractère personnel, ou au cas où il s'est engagé à traiter toutes les données du client comme si elles étaient à caractère personnel, le fournisseur accepte la responsabilité du sous-traitant au sens de la directive 95/46/CE. En outre, pour tout traitement qu'il exécute ou dont il prendrait l'initiative (sauvegarde, transferts, exportation, stockage), le fournisseur accepte d'être tenu par les obligations du responsable du traitement au sens de la directive 95/46/CE.	Rattachement au droit en vigueur
Confidentialité	Quelle que soit la nature des données, le fournisseur s'engage à maintenir une stricte confidentialité des données. Vis-à-vis du client, il est directement responsable des actes de tous ses préposés et des sous-traitants éventuels auxquels il confierait les données.	
Non communication à des Tiers	Sauf si le contrat ou ses annexes prévoient expressément la possibilité de sous-contracter des services, ou un « tiers de confiance » (escrow), le fournisseur s'engage à ne pas communiquer les données à tiers, même pour simple motif de sauvegarde.	
Lieu de traitement et de conservation	Le fournisseur déclare que si des données du client, sont traitées (y compris transférées, conservées ou sauvegardées par lui) ces données resteront localisées et leur traitement soumis à la réglementation : A) Des pays suivants ……* B) Des Etats membres de l'Union européenne et autres pays de l'Espace économique européen (EEE). C) Des pays de l'UE, de l'EEE, et des autres pays repris par la Commission européenne dans la liste des pays offrant un niveau de protection des données suffisant.	Rattachement au droit en vigueur

	D) Des pays sous C) et des Etats-Unis d'Amérique (USA), étant entendu que le fournisseur et tous ses établissements, sous-traitants ou intermédiaires établis dans ce pays et qui pourraient techniquement avoir accès aux données se sont soumis valablement aux règles de l'accord « Safe Harbor » entre l'UE et les USA. (*) choisir et/ou compléter ce qui convient	
Format des données	Au cas où il fournit une plateforme et/ou des applications, le fournisseur garantit que les données sont conservées dans un format standard ouvert (documenté de manière claire et transparente) et libre de droits d'utilisation, en ce sens qu'elles pourront être librement exploitées ou rechargées par le client ou par un autre fournisseur disposant des installations standard requises (par exemple en fin de contrat ou sur demande du client).	Garantie de portabilité
Assurance de restitution des données	En cas de fin de contrat ou sur demande du client, le fournisseur s'engage à restituer au client l'intégralité de ses données, dans le format standard ouvert, documenté et libre de droits ci-dessus, et ce gratuitement ou pour un coût n'excédant pas les frais matériels de réalisation de la copie et/ou du transfert au client. La fin du contrat ainsi que tout différend entre le client et le fournisseur (par exemple suite au non-paiement de factures) peut donner lieu à la suspension ou à l'interruption des services ainsi qu'à tout règlement amiable, arbitral ou judiciaire, mais en aucun cas à une rétention des données par le fournisseur.	Garantie de portabilité
Backup and Recovery	Le fournisseur offre au client les solutions décrites en annexe 5 quant au - backup - redondance - récupération après incident.	
Escrow (option)	Afin d'assurer la disponibilité de ses données pour le client, le fournisseur en placera périodiquement une copie auprès d'un « tiers de confiance ». Le client sera connu des tiers et autorisé à recouvrer sa copie auprès de lui, gratuitement ou pour un coût n'excédant pas les frais matériels de réalisation de la copie et/ou du transfert au client.	
Destruction des données	En fin de contrat et après restitution au client de la dernière copie de ses données, le fournisseur garantit – sauf instruction formelle du client en sens contraire – que les données du client et toutes leurs copies seront effectivement détruites par remise à blanc ou destruction physique des supports, ceci dès que possible et dans un délai maximum de 1 mois.	
Sécurité	Le fournisseur se conforme à des mesures de sécurité, et en particulier il a pris les	Il est difficile de se référer à des

	mesures nécessaires pour : - Protéger physiquement ses installations contre un accès non autorisé ; - Protéger logiquement ses installations contre un accès non autorisé ; - Partager de manière étanche ses ressources entre ses clients ; - Mettre ses infrastructures, plateformes et/ou applications au dernier niveau de sécurité approprié, dans le délai recommandé par leur concepteurs ; - Mettre en place une authentification mutuelle entre ses services et les utilisateurs de son client et gérer ainsi les identités et accès ; - Mettre en place un dispositif de sauvegarde (décrit en annexe 5) ; - Mettre en place un dispositif de cryptage des données (décrit en annexe 6) ; - Mettre en place une traçabilité des accès aux données personnelles (décrite en annexe 7) ; - Mettre en place un système d'alerte et de repérage des incidents ; - Répertorier et documenter les incidents survenus, et les communiquer le cas échéant selon les procédures mises en place par une autorité de contrôle ; - Procéder à une évaluation spécifique et détaillée par priorité des risques qui concernent ses services ; - Mettre en place les mesures nécessaires pour couvrir ces risques, selon leur priorité ; - Faire auditer son évaluation et les mesures mises en place par un spécialiste indépendant.	standards précis (nombreuses normes, évolutives), mais on peut se référer à une annexe
Conformité aux standards	Le fournisseur reconnait son obligation générale de donner l'assurance à son client que son organisation interne et ses procédures de traitement des données sont conformes aux standards nationaux et internationaux applicables. En particulier, il déclare que ses services sont conformes aux standards énumérés en annexe 8.	
Traçabilité	Le fournisseur effectuera des opérations de traçage ou d'audit (logging and auditing) des traitements relatifs aux données à caractère personnel qui sont effectués par lui (ou par ses sous-contractants si applicable/autorisé).	
Signalement d'incidents	Le fournisseur s'engage à signaler et documenter à son client tout incident relatif : - à un problème de sécurité (divulgation, etc.) qui peut concerner directement les données de son client ; - à un problème ou incident sérieux qui peut impacter l'ensemble de ses	

	services, même s'il ne parait pas que les données du client aient été concernées ou affectées.	
Signalement d'autres événements	Le fournisseur s'engage à signaler à son client toute intervention de tiers (par exemple un sous-contractant, un changement d'escrow) au cas où ce tiers pourrait jouer un rôle dans le traitement ou la conservation des données du client. De même, le fournisseur signalera au client tout changement significatif concernant le service, tel que la mise en place de fonctionnalités additionnelles.	
Audit par le client	Le client a le droit de demander, à ses frais, un audit indépendant des procédures de sécurité mises en place par son fournisseur, de sa conformité aux standards déclarés et des incidents éventuels survenus. Le fournisseur s'engage à collaborer à cet audit et à fournir à l'auditeur les informations nécessaires à l'accomplissement de sa mission.	
Notification de demandes d'accès	Le fournisseur notifiera au client toutes les demandes d'accès aux données auxquelles il est légalement obligé de répondre, faites par les autorités judiciaires ou policières compétentes, sauf si cette notification est interdite par la loi, par exemple dans le but de préserver la confidentialité d'une enquête criminelle.	
Assistance au client	Le fournisseur portera une assistance effective à son client pour faciliter l'exercice par les personnes concernées de leur droit d'accès, de rectification ou de suppression de leurs données, et autres interventions techniques qui résulteraient du rôle de « responsable du traitement » joué par le client aux termes de la directive 95/46 CE.	
Exportation de données à caractère personnel par le fournisseur	Au cas où, suivant la déclaration formelle du client et/ou l'engagement du fournisseur, les données conservées par le fournisseur sont des données à caractère personnel au sens de la directive 95/46/CE et sont transférées à l'initiative du fournisseur vers des installations situées dans des pays tiers qui n'assurent pas un niveau adéquat de protection des données, le fournisseur assumera conjointement vis-à-vis du client les obligations de l'*exportateur* et de *l'importateur* de ces données, au sens des clauses contractuelles types (sous-traitants) publiées par la Commission européenne par sa décision du 5 février 2010 (JO 12.2.2010 L39/5) aux fins de l'article 26, paragraphe 2 de la directive 95/46/CE.	On adapte ainsi au cloud les clauses contractuelles types en évitant de les reformuler

10 Tableau des principaux acteurs actifs

Un tableau des principaux acteurs actifs dans le domaine du *cloud computing* en Belgique a été établi, sur base du groupe informel « Belgian *cloud* » et d'autres sources. « En Belgique » ne veut pas dire « belge » : les compagnies citées ont au moins un site ou un représentant en Belgique. La réalité du Benelux fait que certaines compagnies étrangères connues (notamment américaines, on pense par exemple à Amazon) ont choisi d'opérer en Belgique depuis la ville de Luxembourg (ou depuis Amsterdam) et n'ont pas de bureau ni de représentant établis en Belgique.

Le tableau reprend :

- Le nom de l'acteur (par ordre alphabétique) ;
- Son « slogan », la manière – généralement choisie par lui ou tirée de son site – dont il résume son activité auprès de ses clients ;
- Ses principaux services ;
- Le site Web ;
- Le pays et le type (large ou PME). Vu le manque de données publiées et les fréquents achats de sociétés belges par des sociétés étrangères, ces dernières informations sont communiquées sous réserve.

Nom	Slogan	Services	Site	Pays	Type
Altimate	Smart IT distributor	Value-added Enterprise IT solutions Close to its partners expectations Competence and expertise in IT infrastructure solutions	http://www.altimate.be/ Belongs to dcc.ie. Aquired by Arrow Electronics in 2012	?	?

Nom	Slogan	Services	Site	Pays	Type
Amplidata	Build cost-efficient and highly available storage *cloud*s with AmpliStor	Erasure coding ensures reliable data storage Reduces TCO with up to 70 % compared to traditional systems Cuts power usage by up to 90 %	www.amplidata.com	BE	Large (USA & Egypt)
Adc Antwerp	Is ready to serve you!	Tier 3 Carrier Neutral datacenter Pay-as-you-grow model Disaster Recovery	http://www.antwerpdc.be	BE	PME
Arxus	Hosted Service Provider	Hosted Messaging and Collaboration platform Hosted SharePoint Services	www.arxus.eu	BE	PME
Aspex	Hosting your applications	Trouble-free updates Extremely fast deployment Easy support	www.aspex.com	US	PME (35 highly qualified staff members)
Azlan	Part of the Tech Data Group	Converged Infrastructure Data Centre and Virtualisation Unified Communications and Collaboration	www.azlan.com	UK	Part of TechData since March 2003

Nom	Slogan	Services	Site	Pays	Type
Belgacom	Be*Cloud*, providing you end-to-end *Cloud*solutions	We offer *cloud* choice & competences. Private, public or hybrid X-aaS, onsite or hosted in our state-of-the-art datacenter Realising, cost reduction, improved time to market, going green, pay per use	www.belgacom.be	BE	Large
Brandfractal	Social Media Monitoring en Measuring	Impact analysis Sentiment monitoring Community Building	www.brandfractal.com	BE	?
Caligo	*Cloud* Enabling & Migration	Housing & Co-Location Hosted Services *cloud* Services, IaaS,SaaS,PaaS	www.caligo.be	BE	?
Channel Reflex	*Cloud* Go-To-Market	Succeeding in the *cloud* partner eco-system Strategic & operational B2B channel development Individual personalized approach and 2 days *cloud* Training	www.channelreflex.com	BE	PME <10 employees
Cisco	The people are the network	Borderless Network Collaboration Datacenter & Virtualisation	www.cisco.com	US	Large
Citrix	Making *cloud* computing Enterprise-Ready	Protect sensitive data in the *cloud* Develop and test applications in the *cloud* Deliver applications and desktops on demand	www.citrix.com	US	Large

Nom	Slogan	Services	Site	Pays	Type
Clevver	Managed BI services	Rapid Deployment Increased user adoption Reduced Cost	www.clevver.com	?	?
*Cloud*time	We change IT as you know it	Improve your customer support Learn how to reduce your IT cost Greater flexibility and scalability; better security and continuity	*http://cloudtime.be/*	*?*	*PME*
Combell	Your host in the *cloud*	More than 30.000 clients almost 1 out of 5 Belgium websites Custom *cloud* Hosting to the needs of your business	www.combell.com	BE	PME
Dinamiqs	VirtualStorm – Full private *cloud* desktops	Private & public *cloud* applications Application streaming for offline usage Data synchronization from within the private *cloud*	http://www.dinamiqs.com/	NL	?
Element 61	Business Intelligence in the *cloud*	BI & data warehousing in the *cloud* *cloud*-based Performance Management Solutions Supporting leading *cloud* platforms	www.element61.be	BE	? 360 MAN Years of experience
EMC^2	Journey into the *cloud*	Architect for the future Drive workforce productivity Reduce operational cost	belgium.emc.com/index.htm?fromGlobalSiteSelect	US	Large

Nom	Slogan	Services	Site	Pays	Type
Eurofiber	Take advantage of the freedom of an open network	The guarantee that the work on our network is carried out according to pre-agreed procedures minimalises the chances of unnecessary incidents and further increases the reliability of our network.	www.eurofiber.com	NL	?
Exclusive Networks	Value Added Distributor	Security, storage and networking technologies IAAS, PAAS, SAAS IP Address Management	www.exclusive-networks.com	FR	Large
First Served	Think beyond hardware	Smart hosting services Stretching limits of classic server hosting Enterprise grade *cloud* platforms	www.firstserved.net	BE	?
Google	Data centers scattered around the world	12 centres in the USA, one in Australia (Sydney), and 3 major known centres in Europe: Eemshaven and Groningen in the Netherlands and Mons (St. Ghislain), Belgium. Services: Gmail, Google docs, Google+, search engine	www.google.com/about/datacenters/locations/st-ghislain/	US	Large
Hitachi	Data Drives our World	Virtualized Automated Sustainable	www.hitachi.com	JP	Large

Nom	Slogan	Services	Site	Pays	Type
Housing Center	Datacenter- en Netwerkdiensten	Collocation of servers and other infrastructure hardware in fully redundant datacenters *cloud* environment spreading over three datacenters with separate Backup/Disaster Recovery location Managed Services ranging from Basic Server Management to Advanced System Management, Migration and Performance Audits	www.hostcenter.com	CH	?
HP	Take service delivery to the next level	Solutions that help you build *cloud* services Software and services that help you manage and secure your environment Services that help you transform your infrastructure	www.hp.com	US	Large
IBM	The *cloud* – Plan, Build & Deliver	Reduce cost Improve service delivery Enable business innovation	www.ibm.com	US	Large

Nom	Slogan	Services	Site	Pays	Type
Impro Biz	Improve your business	Implementation services for Salesforce CRM Development of applications on force.com and VMforce.com platform Designed to rapidly meet changing business needs	www.improbiz.be	BE	?
InterAct	Making the Data Center work	Virtualisation & *cloud* computing Experts in Data Center Solutions Designed to rapidly meet changing business needs	www.interact-eu.net	EU ?	?
Interxion	Your carrier-neutral datacenter	High density housing Superior Connectivity Belgium's biggest *cloud* hub	www.interxion.com	UK	?
iRelate	Your expert in business relationships	Providing in depth customer insights for better informed decisions Expert in CRM with competence center in Belgium & The Netherlands, servicing both local and international companies Oracle Belux Partner of the Year – Applications 2010 and 2011	www.irelate.be	BE	?

Nom	Slogan	Services	Site	Pays	Type
Kappa Data	Value Added Distributor in Networking & Security	Delivering all components for secure transition in the *cloud* Offering tools to maximize *cloud* performance Applying strong user authentication	www.kappadata.be	BE	?
LaCie	Made for ideas	We offer *cloud* choice : Private, public or hybrid Broad network of competent Storage Partners Specialized in SMB offerings	www.lacie.com	US	Large
LCL	The Belgian *cloud* datacenter	A Carrier Neutral Tier 3 data center LCL likes to find with you the right solution LCL, a flexible building for all your *cloud* computing needs	www.lcl.be	BE	?
Microsoft	*Cloud* Power	Create, Investigate, Transform, Collaborate, Scalability Office 365 Windows Azure & Hyper-V	www.microsoft.com	US	Large
NetApp	The *Cloud*s Are Within Your Reach	Delivering on the Promise of a Virtualized Data Center Perform self-service recoveries in minutes, not hours Provision resources on the fly to meet business needs	www.netapp.com	US	Large

Nom	Slogan	Services	Site	Pays	Type
Nucleus	Specialized in *cloud*-Hosting	Hosting Solution Builder *cloud* Hosting specialist Serious Geeks	www.nucleus.be	BE	?
Oracle	Technology That Powers the *cloud*	Ensure that *cloud* computing is fully enterprise grade Deliver most complete PaaS and IaaS product offerings Develop and enable rich SaaS offering	www.oracle.com	US	Large
ProAct	We secure mission-critical information	Data and Storage centric approach for cost efficiencies Gradual transition and migration to the *cloud* Private, public and hybrid Enterprise *cloud* services	www.proact.eu	SE	?
RES Software	Making the Desktop dynamic	Reduce desktop complexity Manage and deliver secure,personalized and compliant desktops Dynamic workforce with on-demand access	www.ressoftware.com	US	?

Nom	Slogan	Services	Site	Pays	Type
Riverbed	The IT performance company	Increasing application performance with WAN optimization solutions from Riverbed. Eliminating the need to increase bandwidth, storage or servers Delivers greater productivity and cost savings	www.riverbed.com	US	Large
Roger that.net	Enable business process automation through rich mobile interactions	Rogerthat, the world's first "multiple choice messaging platform" Revolutionises communication and process automation via smartphones and tablets We offer our customers flexible mobile reach	www.belgiumcloud.com/?page_id=4684	BE	?
SAAS45 Channel	The *cloud*-SaaS Channel business community	Dedicated online channel community Develop and share knowledge within the ICT Value chain	www.saas4channel.eu	BE	?
SaaSForce	*Cloud* Services Distributor	Marketplace for resellers with real-time provisioning Private, Public, Vendor *cloud* Connections Enable Deliver Manage	www.saasforce.be	BE	?

Nom	Slogan	Services	Site	Pays	Type
SafeNet	The Data Protection Company	Leading global provider of data protection. For over 25 years, global corporations and government agencies have turned to SafeNet to secure and protect their most valuable data assets and intellectual property.	www.safenet-inc.com	US	Large
Silver Peak	Move More. Go Farther. Spend Less	◦Provides Data Center class WAN optimization solutions. ◦Enabling high-quality, reliable throughput over any WAN connection. ◦Optimize all applications and protocols using either physical or virtualized appliances	www.silver-peak.com	US	Large
Symantec *cloud*	Bringing certainty to the exchange of business information	◦Hosted Messaging And Web Security Management ◦Hosted Endpoint Protection ◦Anti Virus & Anti Spam	www.symantec.com	US	Large
Systemat	Bring trust in the *cloud*	◦Local *cloud* integrator ◦Thousands of mid-market customers in Belgium & Luxembourg ◦Green certification ISO 14001	www.systemat.com	BE	Large

Nom	Slogan	Services	Site	Pays	Type
Telenet	Your IT in reliable hands	◦Build your own custom virtual servers ◦Latest hardware in our high-tech data centres ◦Quick interventions for 99,9 % uptime	www.telenet.com	BE	Large
Terremark	Infrastructure as a Service	◦Enterprise *cloud* ◦Infinistructure ◦Managed Dedicated Hosting	www.terremark.be	US	Large
The CRM-Warehouse	*cloud* Integrators	◦Full automation with *cloud* Applications (CRM, HMC, CCM, ERP, CMS) ◦Fixed Fee per month per user ◦100% *cloud*, 100% Customised	www.crm-warehouse.be	BE ?	?
Thin *factory*	Delivering *cloud* Solutions in a Dynamic World	◦*cloud* Infrastructure ◦Marketplace for *cloud* Services ◦*cloud* Orchestration Platform	www.thinfactory.com	BE	?
uptime Group	ICT Differently	◦Your idea our business ◦Power & Passion ◦Knowledge Datacenter	www.uptime.be	BE	?
Vasco	MYDIGIPASS.COM – Join today!	◦Add Convenient Security to your Web Applications ◦Eliminate password management hassles ◦Free mobile client authenticators	www.vasco.com	US	Large

Nom	Slogan	Services	Site	Pays	Type
VM WARE	Accelerate IT. Accelerate your Business	◦Self Service for the *cloud* ◦Scalability & Flexibility ◦Pooling & dynamic resourcing	www.vmware.com	US	?
Xaop	We keep your documents in the *cloud* in Sync & Secure	◦System integration in the *cloud* ◦(Mobile) Application development ◦Process analysis and prototyping	www.belgiumc*loud*.com/?page_id=133	BE	?
Zenith	Zenith Infotech Europe	◦*cloud* oplossingen voor KMO's ◦Private *cloud* ◦Business Continuïteit	www.zenithinfotech.com	US	Large

11 Bibliographie

United Kingdom – Information Commissioner Office (ICO), Guidance on the use of cloud computing, [Online]
http://www.ico.org.uk/about_us/research/~/media/documents/library/Data_Protection/Practical_application/cloud_computing_guidance_for_organisations.ashx

United Kingdom (UK) Open Standards Principles: For software interoperability, data and document formats in government IT specifications [Online]
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/78892/Open-Standards-Principles-FINAL.pdf

Interxion Europe-wide survey of current and intended cloud usage and attitudes towards cloud computing. [Online] http://www.interxion.com/cloud-insight/index.html.

Dale Vile, Freedom Dynamic ltd, A vision for the Data Centre – The Register – [Online]
https://www.google.be/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&sqi=2&ved=0CDgQFjAB&url=http%3A%2F%2Fwhitepapers.theregister.co.uk%2Fpaper%2Fdownload%2F2674%2Fa-vision-for-the-data-centre.pdf&ei=DzZdUf-TJsiQrQfTkICYDw&usg=AFQjCNGrbACIU8jp1mtMGGInnjEFQmcu9A&sig2=u4uILFYBJltPkVS7uEtbUQ&bvm=bv.44770516,d.bmk

European Parliament – DG Internal policies, Fighting cybercrime and protecting privacy in the cloud (study) December 2012 – [Online]
http://www.europarl.europa.eu/committees/en/studiesdownload.html?languageDocument=EN&file=79050

European Commission – COM (2012) 529, Unleashing the Potential of Cloud Computing in Europe [Online]
http://ec.europa.eu/information_society/activities/cloudcomputing/docs/com/com_cloud.pdf
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SWD:2012:0271:FIN:EN:PDF

European Commission COM (2012) 11 Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [Online]
http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=en&DosId=201286

European Commission COM (2011) 942 COMMISSION COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, A coherent framework for building trust in the Digital Single Market for e-commerce and online services [Online]
http://ec.europa.eu/internal_market/e-commerce/docs/communication2012/COM2011_942_en.pdf

European Commission COM (2002) 16 EC Commission Decision of 27 December 2001 on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC. [Online] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002D0016:EN:NOT & http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:FR:PDF

IDC, Quantitative Estimates of the Demand for Cloud Computing in Europe and the Likely Barriers to Up-take - SMART 2011/0045 [Online] http://ec.europa.eu/information_society/activities/cloudcomputing/docs/quantitative_estimates.pdf

ARTICLE 29 DATA PROTECTION WORKING PARTY, Opinion 05/2012 on cloud computing [Online] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf

European Commission – DG INFSO Expert Group Report, The Future of Cloud Computing, Opportunities for European Cloud Computing beyond 2010. [Online] http://ec.europa.eu/information_society/newsroom/cf/itemdetail.cfm?item_id=6993

Neelie Kroes Vice-President of the European Commission responsible for the Digital Agenda Setting up the European Cloud Partnership World Economic Forum Davos, Switzerland, 26th January 2012. [Online] http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/38&format=HTML&aged=0&language=EN&guiLanguage=en.

Cloud Computing: Benefits, Risks and Recommendations for Information Security. [Online] https://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment.

ENISA, Critical Cloud Computing – a CIIP perspective on cloud computing services – December 2012 [Online] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/critical-cloud-computing

ENISA Cloud Computing Information Assurance Framework. [Online] 2009. http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-information-assurance-framework.

ENISA. Security and Resilience in Governmental Clouds. [Online] 2011. http://www.enisa.europa.eu/activities/risk-management/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds/.

ENISA, Cloud Computing, Benefits, risks and recommendations for information security (November 2009) [Online] https://resilience.enisa.europa.eu/cloud-security-and-resilience/publications/cloud-computing-benefits-risks-and-recommendations-for-information-security/view

ENISA Procure Secure – A guide to monitoring of security service levels in cloud contracts [on line] https://www.google.be/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&sqi=2&ved=0CDA

QFjAA&url=http%3A%2F%2Fwww.enisa.europa.eu%2Factivities%2FResilience-and-CIIP%2Fcloud-computing%2Fprocure-secure-a-guide-to-monitoring-of-security-service-levels-in-cloud-contracts%2Fat_download%2FfullReport&ei=yi9dUbWtIcjZrQep5oCYBA&usg=AFQjCNGWddPe5UXWfuBNK1_rRxu0FyaJsQ&sig2=N_sRgVmVd-i9NpRpYnFoGw&bvm=bv.44770516,d.bmk

Information commissioner and Cloud security alliance Slovenian chapter, Personal data protection and cloud computing, (15 June 2012)

NSAI (Ireland) SWiFT 10:2012 Adopting the Cloud – decision support for cloud computing (4 avril 2012) [Online] http://www.nsai.ie/Special-Pages/News/NSAI-and-IIA-Cloud-Computing-Standard-Launched-by-.aspx

Survey and analysis of security parameters in cloud SLAs across the European public sector. [Online] 2011. http://www.enisa.europa.eu/activities/application-security/test/survey-and-analysis-of-security-parameters-in-cloud-slas-across-the-european-public-sector.

International Standard on Assurance Engagements (ISAE) 3402. [Online] http://www.ifac.org/sites/default/files/downloads/b014-2010-iaasb-handbook-isae-3402.pdf.

Cloud Security Alliance Cloud Controls Matrix. [Online] https://cloudsecurityalliance.org/research/ccm/.

Guidelines on information security controls for the use of cloud computing services. [Online] http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=43757. A guide to monitoring of security service levels in cloud contracts

NIST Definition of Cloud Computing - NIST SP 800-145. [Online] http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

NIST. Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. [Online] 2011. http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf.

Government, US. Federal Risk and Authorization Management Programme - Concept of Operations (Includes a section on continuous monitoring). [Online] 2012. http://www.gsa.gov/graphics/staffoffices/FedRAMP_CONOPS.pdf.

Annual FISMA Reporting: Chief Information Officer Questions. [Online] 2009. http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_fy2009/cio_questions.pdf.

ENISA. Resilience Metrics and Measurements: Technical Report. [Online] 2011. http://www.enisa.europa.eu/activities/res/other-areas/metrics/reports/metrics-tech-report.

Commission decisions on the adequacy of the protection of personal data in third countries. [Online] http://ec.europa.eu/justice/policies/privacy/thridcountries/index_en.htm.

European IT decision-makers and influencers give their views on cloud computing. [Online] http://www.interxion.com/cloud-insight/index.html.

Survey and analysis of security parameters in cloud SLAs across the European public sector. [Online] http://www.enisa.europa.eu/activities/application-security/test/survey-and-analysis-of-security-parameters-in-cloud-slas-across-the-european-public-sector.

Survey and analysis of security parameters in cloud SLAs across the European public sector. [Online] http://www.enisa.europa.eu/activities/application-security/test/survey-and-analysis-of-security-parameters-in-cloud-slas-across-the-european-public-sector.

Security and Resilience in Governmental Clouds. [Online] http://www.enisa.europa.eu/activities/risk-management/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds/.

ENISA Cloud Computing Information Assurance Framework. [Online] http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-information-assurance-framework.

Cloud Computing: Benefits, Risks and Recommendations for Information Security. [Online] https://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment.

12 Glossaire des sigles

BCR	Binding Corporate Rules (règles d'une entreprise, soumise à validation par une autorité nationale compétente pour la protection des données)
CIP	Critical Infrastructure protection
CIIP	Critical Information Infrastructure Protection (Eur Commissions Communication on…)
DDoS	Distributed Denial of Service
ECP ou PEC	European Cloud Partnership / Partenariat européen pour le cloud
EEE	Espace économique européen (UE + Norvège, Islande, Liechtenstein)
ENISA	European Network and Information Security Agency
ETSI	Institut européen des normes de télécommunication
IaaS	Infrastructure as a Service (cloud proposant de la puissance de communication, de calcul et de stockage)
LVP	Loi (Belgique) du 8 décembre 1992 relative à la Protection de la vie privée
NIST	(US) National Institute for Standards and Technology
PaaS	Platform as a Service (cloud proposant une plateforme opératoire permettant d'héberger des services)
PME	Petite et moyennes entreprises (< 250 personnes en Europe)
RA	Risk Assessment – Le fait de déterminer quelles sont les infrastructures critiques, leur importance, les incidents à éviter pour elles
SaaS	Software as a Service (cloud proposant des applications ou solutions auxquelles les utilisateurs accèdent en ligne)
SLA	Service Level Agreement (Contrat de niveau de service)
SOA	Service Oriented Architecture
SPF / FOD	Service public fédéral / Federale OverheidsDienst
TCO	Total cost of ownership (coût global d'installation, exploitation et évolution/sortie d'une solution)
UE	Union européenne

© Female photographer - Fotolia.com

economie
SPF Economie, P.M.E., Classes moyennes et Energie

Rue du Progrès 50
1210 Bruxelles
N° d'entreprise : 0314.595.348
http://economie.fgov.be